SIEM

SECURITY INFORMATION & EVENT MANAGEMENT

Introduction to Fundamental Of Networking

Network:

When two or more than two electronic devices are communicating through wired or wireless media for the purpose of communicating data electronically, that is called network.

Networking:

Networking is a concept of communicating digital devices with each other through wired or wireless media for purpose of communicating data electronically.

Internet:

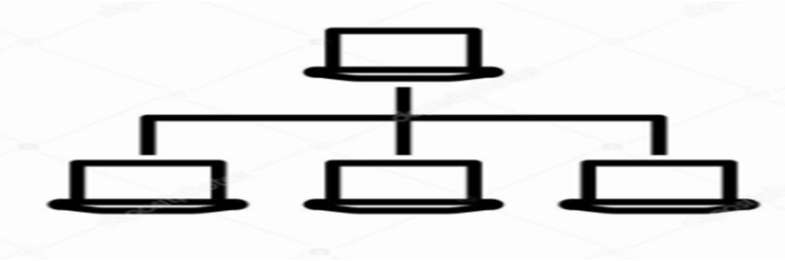
When different networks are interconnected with each other globally or interconnected to public network through ISP for the purpose of sharing and receiving information from web servers that is called Internet.

Type of Network:

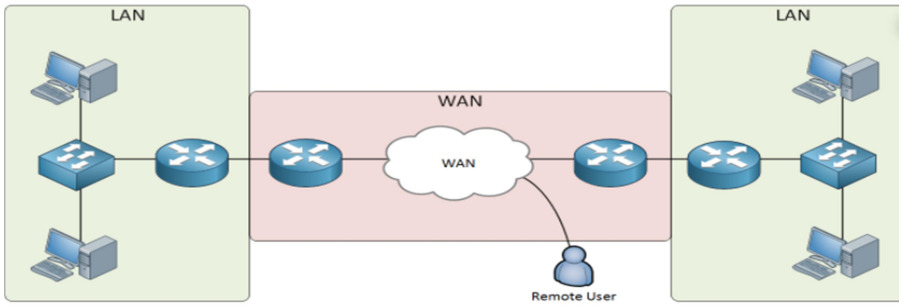
There are mainly three type of network as follows-

LAN (Local Area Network): LAN is a network that interconnects computers through hub or switch within a limited area under control of single organisation.

Wi-Fi and Ethernet is the most common LAN technology.



WAN (Wide Area Network): WAN is a large area network in which network devices are interconnected through Routers and ISP's to globally under control of several organization.



MAN (Metropolitan Area Network): When more than one Local Area Network of same organisation are interconnected through Router but not to public network is called Metropolitan Network.

Network Devices:

1- **Personal Computer/Laptop-** A computer is an electronic device that manipulates information, or data. It has the ability to store, retrieve, and process data.

2- **Server-** A server is a centralized computer hardware or software that provides functionality to the other programs or devices, called "client".

Database servers, File servers, Mail servers, Print servers, Web servers, Game servers, and Application servers are the example of server.

3- **Switch (Layer 2 device works on MAC)-** A switch is a Layer-2 hardware device in a computer network that connects other devices like PCs, printers, Aps, Servers together.

It is an intelligent network device and uses MAC addresses to send data packets to selected destination ports.

It uses packet switching to send, receive or forward data packets from the source to the destination device.

It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.

4- **Multilayer Switch-** A multilayer or Layer 3 switch is basically a switch that can perform routing functions in addition to switching.

5- **Router -** Routers are networking devices operating at layer-3 of the OSI model which provide internetwork communication with the different networks.

Responsible for receiving, analysing, and forwarding data packets from one network to another in the form of IP packets.

It also provides best path selection.

6- **Firewall (Layer3 & 4 works on IP address and Ports)-** A firewall is a network security device either hardware or software based, which monitors all incoming and outgoing traffic and based on a defined set of security rules, it accepts, rejects or drops that specific traffic.

Accept: Allow the traffic
Reject : Block the traffic but reply with an "unreachable error"
Drop : Block the traffic with no reply
We placed hardware firewall between our network and untrusted network (Internet).

There are three type of firewall-

- **Packet Filtering Firewall -** Packet filtering firewall filters the traffic based on source and destination IP address, protocols and ports. Only it can allow or deny the packets based on unique packet headers. It does not check data/payload portion so there may be chances of malicious data.
- **Application/Proxy Firewall-** Application layer firewall can filter the traffic up to application layer(Layer 7) of the OSI model means it checks the data/payload of the received packet. Due to this, it is much slower than packet filtering firewall.

  In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy.
- **Hybrid Firewall-** Hybrid firewalls are the firewalls that have the feature of both the firewalls, are known as NGFW. It provides the security from Advanced malware

attacks and Application layer attack. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

7- **IPS/IDS-** An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flow to detect and prevent vulnerability exploits. Comes in hardware and software both form.

An Intrusion Detection System (IDS) is a network security/threat detection technology that monitors network traffic for suspicious activity and alerts when such activity is discovered.

It works on Layer 3, Layer 4 as well as Layer 7 level.

It is recommended to implement behind the firewall or WAF.

8- **e-Mail Security Appliance-** Email Security Appliance is an email security gateway product which is designed to detect and block a wide variety of email-borne threats, such as malware, spam and phishing attempts.

Cisco Iron Port is an example of e-Mail security appliance.

Characteristics of Network:

Speed: How fast data is being transmitted over the network.

Cost: How much general cost of components, installation and maintenance is cost effective.

Security: How much secure the network.

Availability: Maximum uptime of network for user's use.

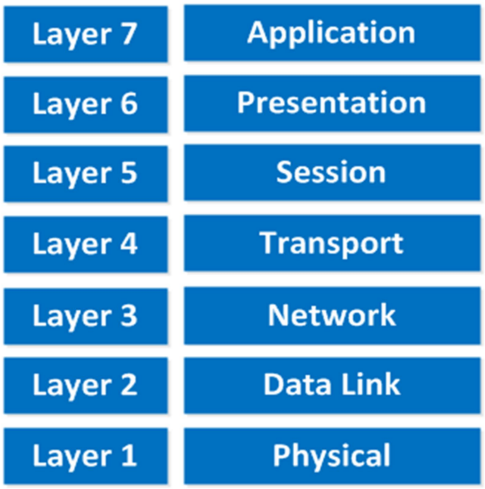
Scalability: Network design for future changing.

Reliability: How much network device are reliable and how long device will work.

OSI Layer Model:

Open System Interconnection Model is a conceptual framework developed by "international Organisation of Standardization" which describes how systems communicate over a network. It allows various type of network devices to intercommunicate so that different vendor's network can interoperate.

It has Seven Layers-



1-Physical Layer: This layer is responsible for actual physical connection between the devices and just sends & receives the data in the form of **bits** (0 or 1).

2-Data Link Layer: The data link layer is responsible for the node to node delivery of the message. This layer makes sure data is formatted in the correct way, takes care of error detection not correction and makes sure data is delivered reliably.

It receives the data in packets, combines the packet into bytes and after that bytes to frames. This concept is called **Framing** or **Encapsulation.**

Frame Contains source and destination mac address.

3-Network Layer: Network layer is responsible for the transmission of data from one host to the other host located in different networks using best path/route and logical addressing (also called Packeting) by placing sender's & receiver's IP address in header.

IPv4 , IP v6.

4-Transport Layer: Transport layer provides services to application layer and takes services from network layer. This layer is responsible for **reliable transfer** of data by ensuring at destination is error free and in order/sequence through **acknowledgement**.

It takes the data from upper layer and forward to next layer after segmenting it and also implements **Flow & Error Control** (Error correction before transmit) to ensure proper data transmission.

It can be Connection Oriented **(TCP)** and Connection Less **(UDP)** communication.

5-Session Layer: The session layer takes care of establishing, managing and termination of sessions between two hosts. If the session is broken then this layer attempt to recover the session. Also keeps different application data separate from other application's data while travelling.

6-Presentation Layer: It presents data to Application Layer in readable format with data transmission and code formatting. It also compress/decompress and encryption/decryption of data.

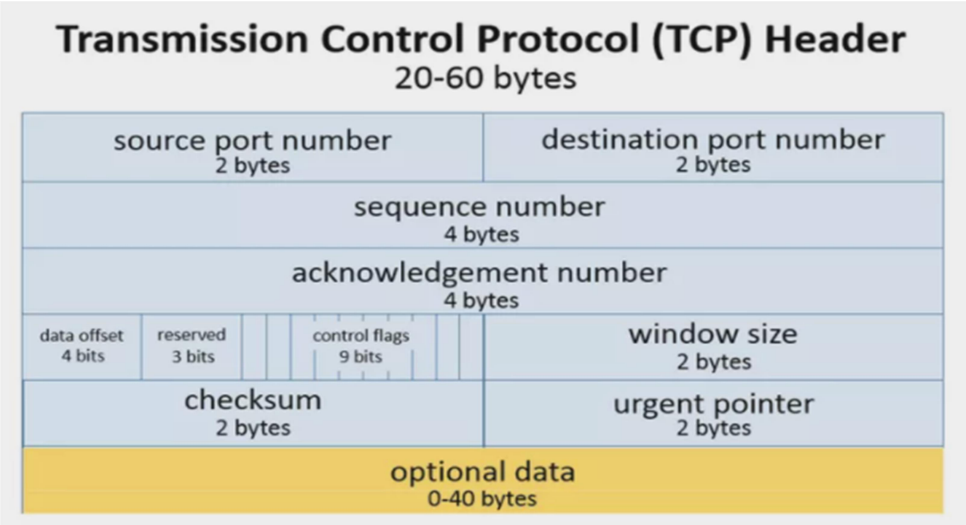
7-Application Layer: This layer provides the interface between user application and the device. Web browser and email client are the example of user application.

ftp, http, pop3, telnet etc.

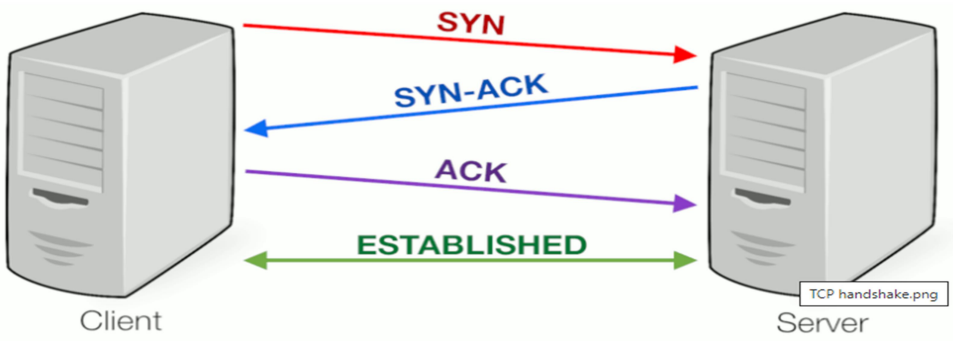
What is TCP Protocol:

TCP stands for Transmission Control Protocol which is a connection oriented and reliable communication protocol which works on layer 4 of OSI model (transport layer). It ensures message reaches its destination successfully and in sequence through **acknowledgement**.

File Downloading, File Sharing, Printing etc.



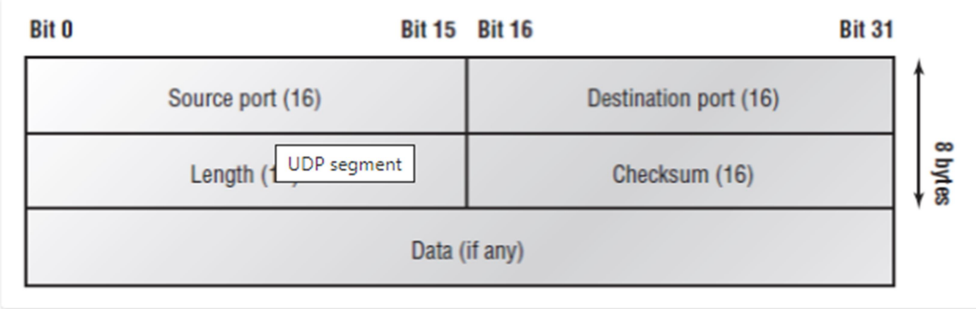
TCP Three Way Handshaking :



What is UDP Protocol:

UDP stands for User Datagram Protocol which is a connection less communication protocol. It provides unreliable & unacknowledged delivery of message to destination.

VoIP, Video Streaming



UDP Segment

Network Ports:

A port is a virtual point where network connections start and end. Network ports are provided by the TCP or UDP protocols at transport layer. Ports are software-based and managed by a computer's operating system. Each port is associated with a specific process or service. Port numbers are used to determine which protocol incoming traffic should be directed to.

Ports use is regulated by the **Internet Corporation for Assigning Names and Numbers (ICANN)**.

Classification of port numbers

The port numbers are divided into three categories:

- **Well-known ports**
- **Registered ports**
- **Dynamic ports**

Port Number Range	Part Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Some Common Ports are-

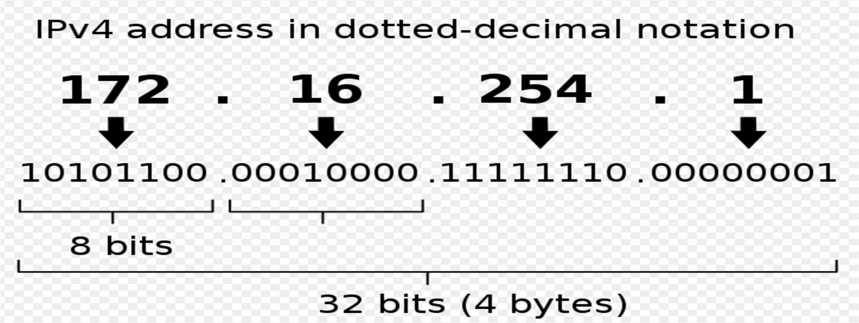
ftp : 20, 21,
ssh: 22
telnet: 23
smtp : 25

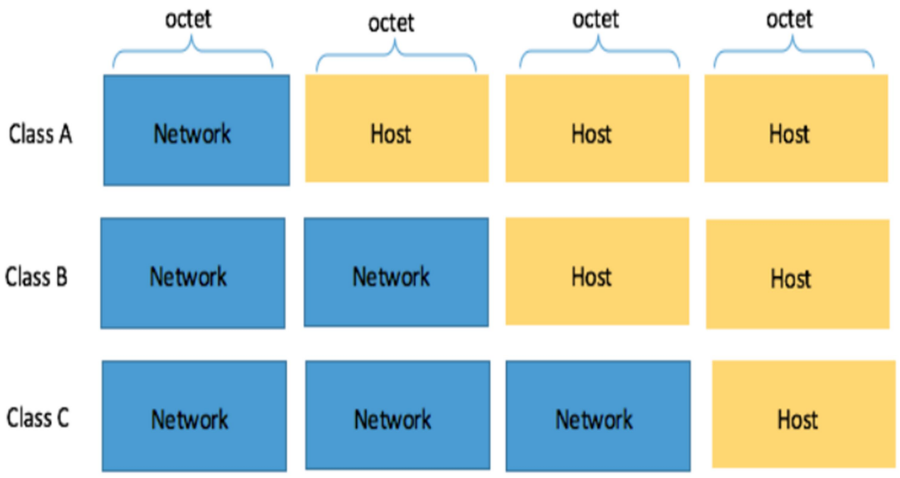
dns: 53
http: 80
https or ssl : 443
rdp : 3389
ntp : 123
imap4 :143
pop3: 110

IP Address V4:

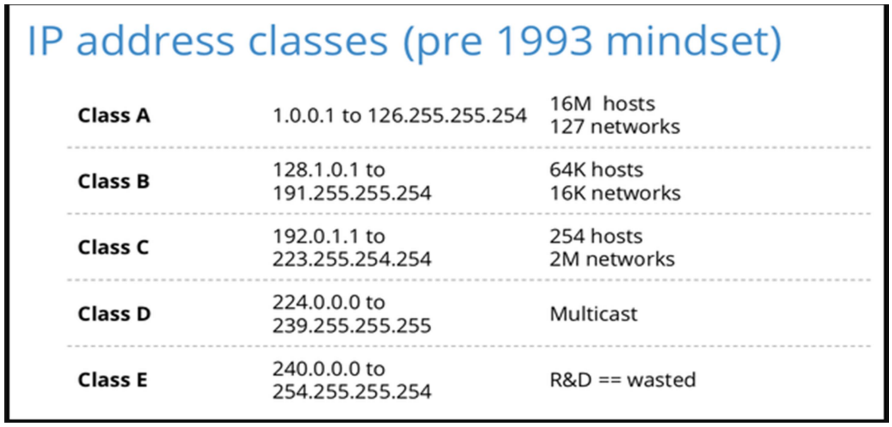
IP is a unique identifier to each device connected to network that uses the IP protocol for communication.

It is a 32 bit logical address (4 octet of 8 bit) which contains network and host part.





IP Address v4 Class Range:



 # 127.0.0.1 is a loopback IP.

Domain Name System:

The Domain Name System is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

DNS translates human readable domain names to machine readable IP addresses.

DNS Records-

- **A Record(Address Mapping Record)-** Known as a DNS host record, The record that holds the IP address of a domain.
- **AAAA Record (IP Version 6 Address record)-** The record that contains the IPv6 address for a domain.
- **CNAME Record (Canonical Name record)-** A canonical name (CNAME) is a record that forwards one domain or subdomain to another domain, does NOT provide an IP address.
- **MX Record (Mail exchanger record)-** Directs mail to an email server.
- **NS Record (Name Server records)** - A name server (NS) record provides a list of the authoritative DNS servers (also called name servers) responsible for the domain that you're querying.
- **PTR Record (Reverse-lookup Pointer records)-** Allows a DNS resolver to provide an IP address and receive a hostname (reverse DNS lookup).

- **CERT Record (Certificate record)-** Stores encryption certificates—PKIX, SPKI, PGP, and so on.
- **SOA record -** Stores admin information about a domain.
- **SRV Record (Service Location)-** Specifies a port for specific services.
- **TXT Record (Text Record)-** Allows admin to store text notes in the record. These records are often used for email security.

  SPF- An Sender Policy Framework record is a DNS TXT record containing a list of the IP addresses that are allowed to send email on behalf of your domain.

  DKIM- Domain Keys Identified Mail (DKIM) is an authentication standard used to prevent email spoofing.

  DMARC- Stands for Domain-based Message Authentication, Reporting, and Conformance is TXT record used by receiving mail servers to determine what to do with a failed message.

  Tell the recipient server to either: Quarantine the message or Reject the message or Allow the message to continue delivery.

  Sends reports to an email address or addresses with data about all the messages seen from the domain.

Introduction to Information System Security

Information Security:

Information security is a concept to protect of both **physical and digital information and information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Cyber Security:

Cyber security is a concept to protect **digital information and information systems** ie: networks, devices, programs, and data from, Cyber Attack, damage, or unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Cyber Security is considered as subset of Information security.

CIA Triad:

Confidentiality, Integrity and Availability, also known as the CIA triad.

Confidentiality- A concept which insures and protect the data from unauthorized access. The data is available only to the intended and authorized person.

Integrity- This concept insures the accuracy and consistency of data. Means make sure that data is reliable and not changed by unauthorized person.

Availability- It make sure that the data, network resources/services are available every time when authorized user require it.

What is Asset:-

Any valuable thing of an organization which can be in the form of software or hardware.

What is Threat:-

A threat is a potential danger or risk to an asset of an organization. It is of two types-

Latent Threat- A threat which is not publically known is called Latent Threat.

Realized Threat-Realized threat are the threat which are publically known but still hack able even after patch issued due to patch not applied, is called realized threat.

What is Malware:

Malware is a threat in form of a malicious software or code which is intentionally designed to cause damage of computer, server or computer network.

What is SPAM eMail:

Spam email is unsolicited and unwanted junk email sent out in bulk to a recipient list sent for commercial purposes.

What is eMail Spoofing:

Email spoofing is a form of cyber-attack in which a hacker sends an email that has been manipulated to seem as it originated from a trusted source.

What is Attack: A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into two categories-

Web based attack and System based attack.

Web based attack- These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

- **Injection attacks-** It is the attack, in which some data will be injected into a web application to manipulate the application and fetch the required information.
  Example- SQL Injection, Code Injection, Log Injection, XML Injection etc.

- **DNS Spoofing-** DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, Exa.- an IP address.

- **Session Hijacking-** It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

- **Phishing-** Phishing is a type of social engineering attack which attempts to steal sensitive information like user login credentials and credit card number.

  Attacker uses forged email contains malicious intended link or attachment tricking the email recipient into believing that the message is something important from their bank, or a note from someone in their company or replica websites of a genuine website as a weapon.

- **Brute Force-** It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.

- **DOS/DDOS-** Dos/DDOS attack is a type of attack making a server, website or resource unavailable to the user It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.

  DOS – Denial of Service – Attack that uses single source to flood a targeted resource.

  DDOS-Distributed Denial of Service- Attack that uses multiple source to flood a targeted resource.

  How to mitigate the DOS/DDOS attack? DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack.

By utilizing specially designed network equipment, we can mitigate the DOS/DDOS attack. Like **Arbor**, a product of **Netscout** and **DefensePro**, a product of **Redware.**

- **Dictionary attacks-** This type of attack stored the list of a commonly used password and validated them to get original password.

- **URL Interpretation-** It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

- **File Inclusion attacks**- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

- **Man in the middle attacks**- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System based attack- These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

- **Virus-** A computer virus is a type of malware or program written to alter the way of a computer operates and is designed to spread from one computer to another by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code.

  In order for a virus to infect your computer, you have to run the infected program.

- **Worm-** Another type of malware which is similar to virus but worms can be spread from computer to computer without any human interfere.

- **Trojan horse-** A type of malware which presents itself as a genuine software and misleads to user but can cause of

serious harms to the systems or computer network by deleting files and destroying the information.

Trojan horse also creates backdoor o computer that gives access of a system to the malicious intended user.

Like virus or worms, it does not self-replicate.

- **Spyware**- A malicious software that aims to gather information of a system installed on that device without the end user's knowledge and permission.

- **Adware**- A malicious software that automatically displays or downloads advertising material such as banners or pop-ups when user is online.

- **Ransom ware**- Ransom ware is also a type of malware which is also known as shareware. This kind of malware can lock down your computer system and threaten to erase everything unless a ransom is paid to the hacker.

- **APT:** APT stands for advanced persistent threat is a network attack in which an unauthorized entity gains access to a network and stays undetected for a long time.
  The intention of an APT attack is to steal the data rather than to cause damage to the network or organisation.

- **Botnet:** Botnet is a network of infected computers that are made to work together under the control of an attacker.

Types of Cyber Attackers:

An attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset by identifying security weakness and using those vulnerabilities.

There are four types of attackers which are as follows-

- **Cyber Criminals**- Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits.

- **Hactivists**- Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology.

- **State Sponsored-** State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin.

- **Insider Threats-** The insider threat is a threat to an organization's security or data that comes from within. These type of threats are usually occurred from employees or former employees.

Hacking:

Hacking is an attempt or activity to compromise and gain unauthorized access to digital devices, networks and data or information by identifying their security weaknesses and using those vulnerabilities.

Hacker:

Hacker is a computer expert who uses his/her technical skill to compromise digital device, network, data or application of an individual or an organization.
Hackers are of different types and are named based on their intent of the hacking system.

Type of Hacker: Basically there are three type of hacker as follows-

White Hat or Ethical Hackers - White Hat Hackers do not intend to harm the system or organization but they do so, officially, to penetrate and locate the vulnerabilities, providing solutions to fix them and ensure safety.

Black Hat – Contrary/Opposite to an ethical hacker, black hat hackers or non-ethical hackers perform hacking to fulfil their selfish intentions to collect monetary benefits.

Gray Hat - Grey hat hackers are the combination of white and black hat hackers. They hack without any malicious intention

for fun. They perform the hacking without any approval from the targeted organization.

Script Kiddie- Do hacking activity for learning purpose.
Cyber Terrorist- Do hacking for national enmities.
Hacktivist- Do hacking activity for their Political moto.

Ethical Hacking:

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization to prevent Cyber Attacks and security breaches by lawfully hacking into the systems and looking for weak points.

Type of Ethical Hacking:

1- Social Engineering
2- Web Application Hacking
3- Web Server Hacking
4- System Hacking
5- Wireless Network Hacking

Red Team V/S Blue Team in Hacking:

Offensive Security - Defensive Security
With Zero info. - With full info. of Infrastructure
Ethical Hacking - Infrastructure Protection
Exploiting Vulnerabilities –Damage Control
Penetration Testing – Incident Response etc.

Phase of Hacking:

1- Information Gathering
2- Scanning
3- Gaining Access
4-Maintaining Access
5-Clearing Tracks

Vulnerability:

It is an exploitable weakness in software, system or in network etc by which cybercriminals gain unauthorized access to a computer system. After exploiting vulnerability, a cyber-attack can run malicious code, install malware and even steal sensitive data.

Zero Days Vulnerability- A zero-day vulnerability is a vulnerability in a system or device that is either unknown or if it has been disclosed but not yet patched. Also known as zero day exploit. Until the vulnerability is mitigated, hackers can exploit it to affect programs, data, computers or a network.

Zero Days Attack- An exploit directed at a zero-day vulnerability is called a zero-day exploit, or zero-day attack.

Vulnerability Management:

Vulnerability management is a cyclical practice of identifying, classifying, remediating and mitigating security vulnerabilities. The essential elements of vulnerability management include **"Vulnerability Detection", "Vulnerability Assessment" and "Remediation".**

Methods of vulnerability detection include:

- **Vulnerability scanning-** A vulnerability scanner is software designed to assess computers, networks or applications for known vulnerabilities.

  VA Scanner can identify and detect vulnerabilities rising from misconfiguration and flawed programming within a network and perform authenticated and unauthenticated scans:

  Authenticated scans: Allows the vulnerability scanner to directly access networked assets using provided system credentials.

  Unauthenticated scans: Result may be false positives and unreliable information about operating systems and installed software. This method is generally used by cyber

attackers and security analysts to try and determine the security posture of externally facing assets and to find possible data leaks.

- **Penetration testing-** Penetration testing, also known as pen testing or ethical hacking, is the practice of testing an information technology asset to find security vulnerabilities an attacker could exploit. Penetration testing can be automated with software or performed manually.
- **Google hacking-** Google hacking or "Google Dork" is the use of a search engine, such as Google or Microsoft's Bing, to locate security vulnerabilities.

Once vulnerability is found, it goes through the vulnerability assessment process:

- **Identify vulnerabilities:** Analysing network scans, pen test results, firewall logs, and vulnerability scan results to find anomalies that suggest a cyber-attack could take advantage of vulnerability.
- **Verify vulnerabilities:** Decide whether the identified vulnerability could be exploited and classify the severity of the exploit to understand the level of risk
- **Mitigate vulnerabilities:** Decide on countermeasures and how to measure their effectiveness in the event that a patch is not available.
- **Remediate vulnerabilities:** Update affected software or hardware where possible.

What is DLP:-

Data loss prevention, or DLP, is a set of technologies, products, and techniques that are designed to stop sensitive information from leaving an organization.

Data can end up in the wrong hands whether it's sent through email or instant messaging, website forms, file transfers, or other means.

O.S. Hardening:

Operating system hardening involves patching and implementing advanced security measures to secure a server's operating system (OS).

What is Proxy:

A proxy server provides a gateway between users and the internet and act as web filters or firewalls to protect computer from internet threats like malware.

Web traffic requests are first sent to the proxy server, which handles the request along with the additional tasks of filtering content, scanning for malware, masking the origin of the request, encrypting messages, and more.

Web Filtering Device- Cisco Umbrella, NGFW

Web Security Appliance - Cisco Web Security Appliance (WSA)

Email Security Appliance- Cisco Iron Port

Bluecoat- Bluecoat Proxy

What is Antivirus:

Antivirus is a kind of software also called end point protection, used to prevent, scan, detect and delete viruses from a computer. Antivirus works based on the latest signature or behaviour of the malware.

There are two type of scan which antivirus do- 1-Real time scan. 2- Scheduled Scan.

Antivirus action if virus found-

1-Clean/Delete - when 100% sure.

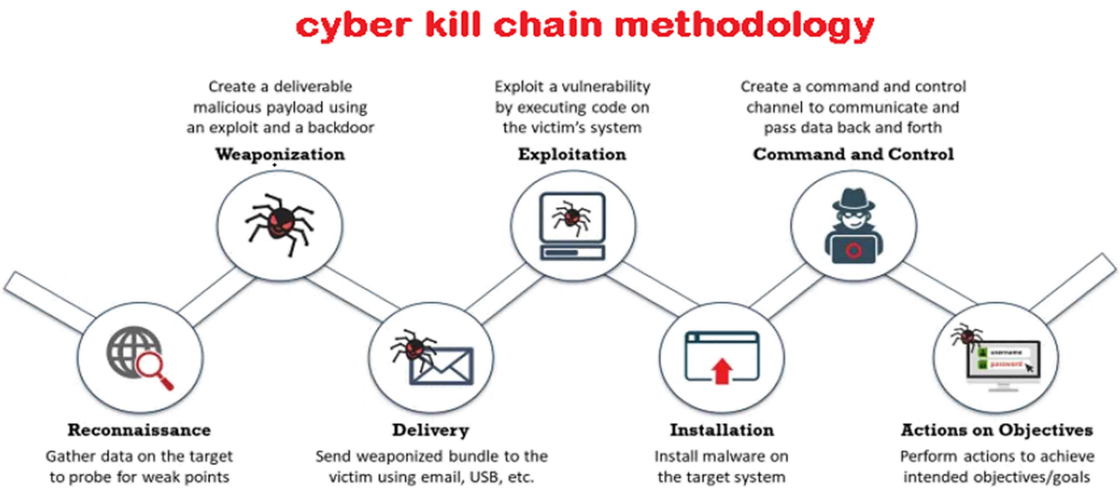
2-Quarantine - when approximately 75% sure.

3- Left Alone – When 50% sure and not able to clean.

Cyber Kill Chain Methodology:

The cyber kill chain is essentially a cyber-security model created by “Lockheed Martin” that traces the stages of a cyber-

attack, identifies vulnerabilities, and helps security teams to stop the attacks at every stage of the chain.



- **Reconnaissance-** An observation stage in which attacker collects data about the target and the tactics for the attack. This includes harvesting email addresses and gathering other information.

  Detect: Web Analytics; Threat Intelligence; Network Intrusion Detection System

  Deny: Information Sharing Policy; Firewall Access Control Lists

- **Weaponization-** Preparing or creating a deliverable malicious payload by attacker using an exploit and a backdoor.

  Detect: Threat Intelligence; Network Intrusion Detection System

  Deny: Network Intrusion Prevention System

- **Delivery-** The attacker delivers the weaponized malware via a phishing email or some other medium. The most common delivery vectors for weaponized payloads include websites, removable disks, and emails. This is the most important stage where the attack can be stopped by the security teams.

  Detect: Endpoint Malware Protection

Deny: Change Management; Application Whitelisting; Proxy Filter; Host-Based Intrusion Prevention System, Router ACL, Trust Zone etc

- **Exploit-** When malicious code is delivered into the organization's system. Exploiting vulnerability by executing that malicious code on the victim's system. It means the perimeter is breached here.

  Detect: Endpoint Malware Protection; Host-Based Intrusion Detection System.

  Deny: Secure Password; Patch Management, Firewall, Trust Zones.
- **Installation-** A backdoor or Remote Access Trojan is installed on the target system by the malware that provides access to the intruder. This is also another important stage where the attack can be stopped using systems such as HIPS (Host-based Intrusion Prevention System).

  Detect: Security Information and Event Management (SIEM); Host-Based Intrusion Detection System

  Deny: Privilege Separation; Strong Passwords; Two-Factor Authentication, Router ACL, Firewall, Trust Zone.

- **Command & Control-** The attacker gains control over the organization's systems and network. Attackers gain access to privileged accounts and attempt brute force attacks, search for credentials, and change permissions to take over the control.

  Detect: Network Intrusion Detection System; Host-Based Intrusion Detection System

  Deny: Firewall Access Control Lists; Network Segmentation

- **Actions on Objective-** The attacker finally extracts the data from the system. The objective involves gathering, encrypting, and extracting confidential information from the organization's environment.

  Endpoint Malware Protection, Incident Response, Data Loss Prevention; Security Information and Event Management (SIEM).

Type of SOC-

As per company to company requirement, SOC is defined in two categories.

In House SOC- In house SOC is the SOC of the company, which manage the security by it's own and has it's own team not outsourced.

Outsourced/MSSP SOC- An outsourced SOC is the SOC of the company which security is managed by Managed Security Service Provider (MSSP), a kind of service based company ie: TCS, Wipro, Accenture etc. who provide security services to it's clients. It can be either Shared SOC or Dedicated SOC.

- **Shered SOC**- If security services are being provided to multiple clients simultaneously then it is called Shared SOC.
- **Dedicated SOC**- If security services are being provided to one client dedicatedly then it is called Dedicated SOC.

OWASP Top 10 Vulnerability-

OWASP stands for the Open Web Application Security Project, is a list of top 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures.

1-Broken Access Control
2-Cryptographic Failures (Sensitive Data Exposure)
3-Injection
4-Insecure Design (New)
5-Security Misconfiguration
6-Vulnerable & Out-dated Components
7-Identification and Authentication Failures (Broken Authentication)
8-Software and Data Integrity Failures (Insecure Deserialization) (New)
9-Security Logging and Monitoring Failures (Insufficient Logging & Monitoring
10-Server Side Request Forgery (SSRF) (New)

Security Information & Event Management

SIEM (Security Information & Event Management):

SIEM is a centralized log management tool which collects real time logs from network devices, security devices, servers, applications, databases etc.

Once it collects the logs, it normalizes (parsed + Normalizes) the logs (means it convert the log from non-readable form to readable format) and keeps the logs for long time for audit, compliance and forensic purposes. As well as it gives searching & reporting feature. It also enables Real time Monitoring. Correlation and Alerting feature.

There are multiple SIEM solutions available in market as follows-

ArcSight	-	Microfocus	
Splunk	-	Splunk Inc.	
Qradar	-	IBM	
ELK Stack	-	OpenSource	etc.

ARCSIGHT

ARCSIGHT :

ArcSight is a well-known SIEM tool managed by vendor Microfocus.

There are major three components of ArcSight. Connector, Logger & ESM.

- **Connector-**

  Connector is a component of ArcSight which is responsible for collecting the Real Time Logs from various devices such as network devices, security devices, servers, applications & databases etc.

Once it collects the logs, it normalizes the log and sends it to Logger and/or ESM. ArcSight receives logs in Event per Second (EPS).

Connector is available in both the form as Software as well as Hardware.

Software version of Connector can be install only on either Windows version of Servers or CentOS / Red Hat Linux version of Linux Servers. Maximum companies prefer to install it on Windows Server.

Hardware Connector device comes on Linux platform having 30+ type of preinstalled Connector. Hardware Connector name "**ConApp**".

- **Logger-**

Logger is a component of ArcSight which receives the logs from Connector and keeps it for long time based on audit, compliance and forensic requirement. It also enables searching and reporting feature.

It also available in both Hardware and Software model.

We can only install Logger on CentOS or Red Hat Linux.

Logger uses the **Oracle database**.

Logger can hold the logs for long time or in years (ie: 3 years, 5 years , 10 years, etc.) as per business requirement

- **ESM (Enterprise Security Manager)-**

It is a component of ArcSight which can receives the log either from Logger or directly from Connector. It enables Real Time Correlation and Monitoring & Alerting capability.

ESM also available in both Hardware and Software model. Software version of ESM name is **ESM-Manager** and Hardware version of ESM name is **ESM- Express.**

ESM uses “CORR” engine database which stand for “Correlation, Optimization, Retention and Retrieval engine”. Actually base engine is **MySQL database**.

ArcSight can receive or supports up to 1 lakh event per second.

Current Version of Connector, Logger & ESM :

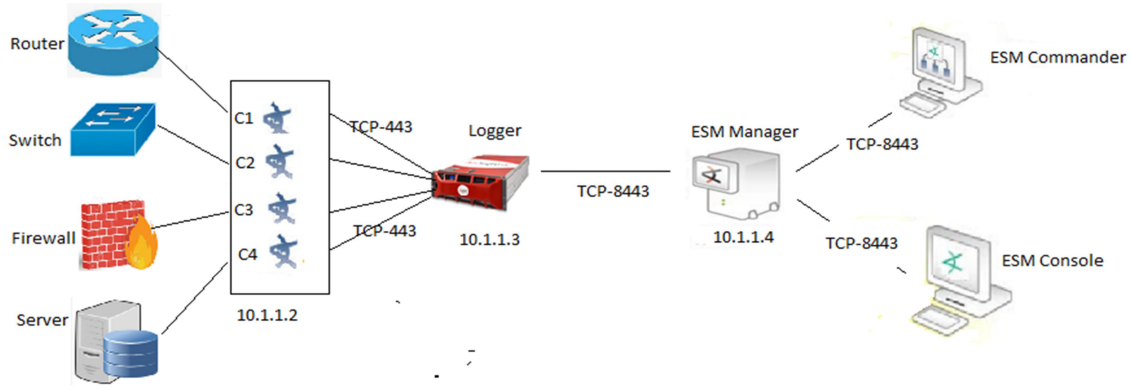
Component Name - Latest Version - Current version in Use

Connector	8.0	7.15
Logger	7.0	6.8
ESM	7.4	7.2

Type of ArcSight Architecture:

There are two type of architecture of ArcSight. First one is Linear and second one is Dual Destination Architecture.

- **Linear Architecture of ArcSight:**



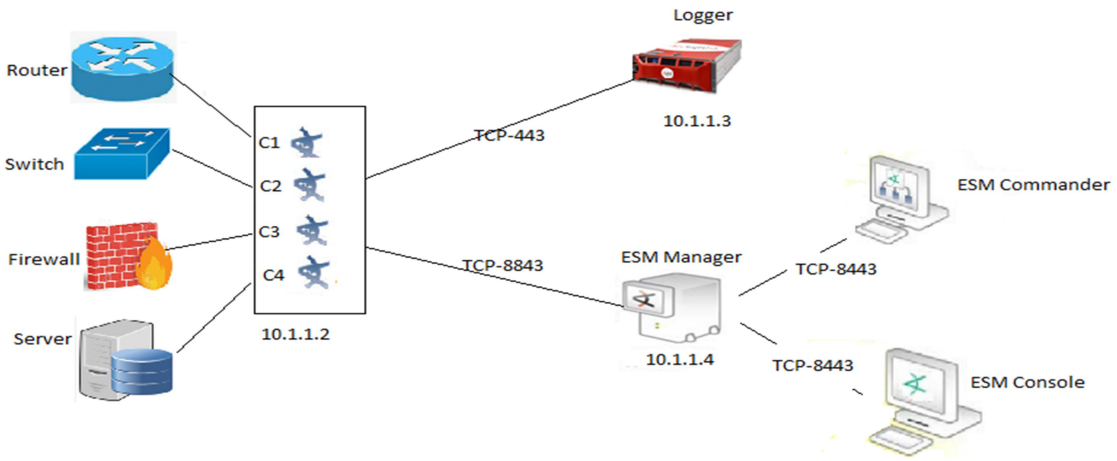
In Linear architecture of ArcSight, Logger and ESM connects in line. Connector sends logs to the Logger and Logger further sends the logs to ESM.

In case of Logger will down or connection between Connector and Logger will down then ESM will not receive logs.

In Linear architecture of ArcSight, it required single bandwidth from the data centre where we have deployed connector server to data centre where we have deployed Logger & ESM.

In Linear architecture of ArcSight, we can't manage the Connector from ESM or Logger.

- **<u>Dual Destination Architecture of ArcSight:</u>**



In Dual Destination architecture of ArcSight, Connector sends one copy of logs to Logger and one copy of log to ESM parallel.

In case of Logger will down or connection between Connector and Logger will down then ESM will still receive the log. In second case if ESM will down or connection between Connector to ESM will down then Logger will still receive the logs.

In Dual Destination architecture of ArcSight, disadvantage is it will require dual bandwidth from the data centre, where we have deployed Connector to data centre, where we have deployed Logger & ESM.

In Dual Destination architecture of ArcSight, Connectors are directly reporting to the ESM so we can manage the Connectors from ESM itself.

(Managing the connectors from ESM means we can check the Connector status weather Connector is running or down, Check the JVM utilization of the Connector as well as EPS of the Connector, can stop, restart and upgrade the connector version. We can also apply the destination setting of the connector such

as cache, batching, aggregation, filtering etc. from the ESM itself.)

How to Access ESM:

There are two ways to access ESM. First one is "ESM Console" and second one is "ESM Command Centre".

- **ESM Console-** ESM Console is a user interface of the ESM using which we can do the Real Time Monitoring, Alerting, writing the Correlation rule, report and dashboard etc.
- **ESM Command Centre –** It is web interface application of ESM which generally used to manage the advanced activity of the ESM such as adding the storage, creating the storage group, setting the retention period and taking the back-up and archive. We can access ESM through below mentioned path-

https://<IP address of ESM>:8443

How Connector Works-

Whenever Connecter receives the raw logs on its input, it does **Normalization** of the logs (In ArcSight Normalization is combination of Parsing and Normalization both. Parsing means breaking down the events).

On its output, it does **Caching, Batching, Aggregation and Filtering.**

- **Normalization-** Mapping of device specific field set into a SIEM specific common field set is called Normalization. In ArcSight common field set is called **Common Event Format(CEF)** which has 300+ field sets.
  There is a file in the connector in which it is defined that which field of device is mapped with which field of ArcSight, that is called **Parser file.**

- **Caching-** Cache memory is a temporary memory or storage of the connecter. By default it is 1GB and we can increase up to 50GB. Connector use Java Virtual Memory (JVM). Default JVM is 256 Mb upgradable to 10Gb.

What are the case when Connector will start the Cache the logs in Cache memory.

1- When Destination (Logger or ESM) is down.

2- When Destination (Logger or ESM) is un-reachable.

3- When Connector is overloaded. It happens when more logs receives compare to JVM.

- **Aggregation-** Aggregation is a destination setting of the Connector which we apply for the devices which are very frequent in sending similar and repetitive event such as Firewall, Router etc.

  For Example: If there are 100 events generated by the device within a specific time such as 5, 10 or 15 seconds (max up to 30 seconds) etc where important fields such as Source address, Destination address, Destination Port, device action are same. Though instead of sending all 100 events, Connector will apply aggregation and send one event with total count of 100 in that specific seconds ie 10 second.

  In another case, if specific time (ie:10 seconds) happened and less than 100 count came (ie: 80 count) it sends one event with total count of 80.

- **Batching-** Batching is one of the destination setting of the Connector which we apply for the devices which are sending different event and slow in sending the events such as windows device instead of doing frequent look-up for the log by the connecter, we can set connecter to hold and wait for the specific set of events and then send.

  For Example: 100 events in 10 Seconds.

- **Filtering-** Dropping of unnecessary events which are not required for security monitoring or forensic purpose is called filtering. It can be apply on the Connector level as well as Logger level.

Advantage of applying of Aggregation, Batching and Filtering:

- To optimize Connector resources such as CPU & JVM.

- To optimize Bandwidth between Connector to Logger and Connector to ESM.
- To optimize storage requirement for the Logger & ESM.
- To optimize License utilization.

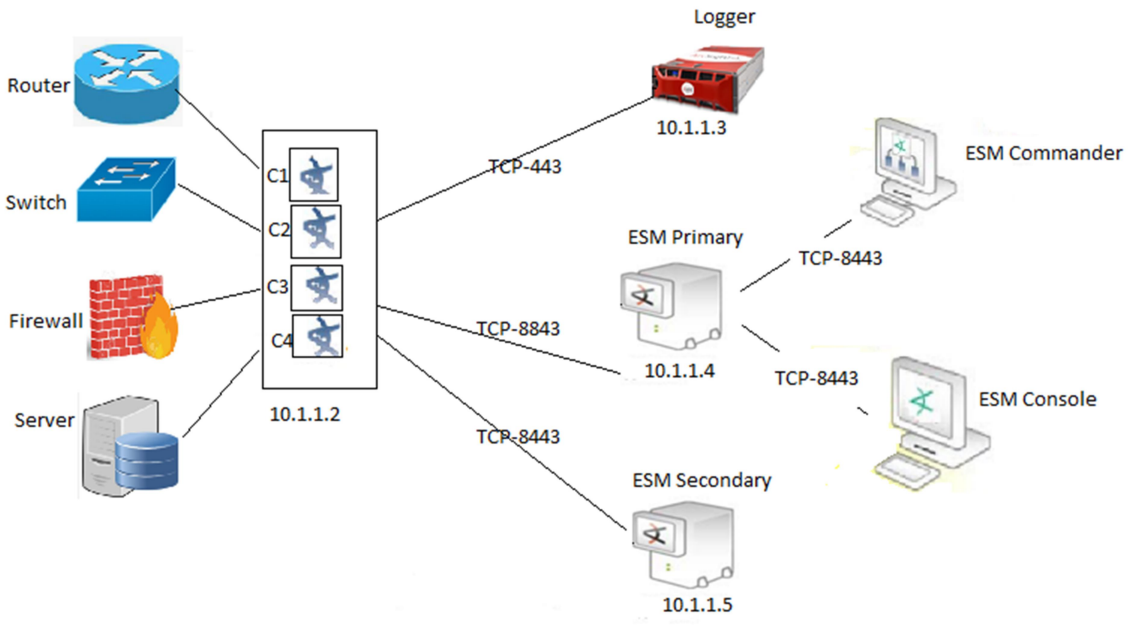
Disadvantage of applying of Aggregation, Batching:

- No Real Time monitoring because logs will not be coming in Real Time due to holding the event for the specific time.

Disadvantage of applying of Filtering:

- No such as any disadvantage of Filtering.

Dual Dest. Arch with High Availability or Failover:



It is an architecture of Dual Dest. Architecture with back-up ESM so that secondary ESM can take place in case of primary ESM is down. So that Real Time monitoring and Correlation will not be impacted.

Logs which were sent to primary ESM will not be available to secondary ESM. If we need to search those logs, we have to search that from Logger.

ArcSight Licensing:

ArcSight is a licensed product of vendor named Microfocus Inc. Logger and ESM both require license. For Connector, license is not required. Logger and ESM license both are comes in EPS (Events Per Second).

How to plan for ArcSight License or ArcSight Deployement Planning:

To plan or buy the license for ArcSight deployment, we required below mentioned details-

1-Device Inventory List- Total device's list which will be integrated to SIEM.

2- EPS Calculation for Logger or ESM- We calculates the approx. EPS count based on device's inventory list or total devices. Calculation happens on 24 hour basis (means how much EPS generated in 24 hours from 12:00AM to 12:00AM in midnight).

For Example: If we find approx. 10000 EPS count then we will plan 20% more than total generated EPS for future perspective. So in respect of 10k EPS, it will be total 12k.

3- Log Retention Period- Maximum time for which log will be available for searching and reporting for auditing or compliance purpose.

Normally ESM keeps the logs for approximately 60 days.

4- Resource Calculation- How much RAM & CPU required for Logger & ESM. Minimum RAM requirement is 64 Gb but it is recommended to go with 128 Gb RAM for ESM. Minimum CPU is required 32 core but recommended 64 core of CPU. We should refer Logger or ESM support matrix document for resource planning.

5- Storage requirement – How much GB storage will required for calculated EPS for one year. We generally use HDD for Logger and SSD for ESM because SSD is much faster than HDD.

6- Connectivity- How much bandwidth with dedicated line.

What will happen when Logger License violated ?

If Logger license is violated, we will see the warning message on the top of the logger console mentioning that "**Your Logger license has been violated one time in this month. If it continues to violate more than 5 times in the month, your logger searching & reporting feature will be disabled. Kindly contact Microfocus sales team to upgrade your license."**

What will happen when ESM License violated ?

ESM license is same as Logger license. Only difference is that ESM does not disable any feature even license violated because it is a critical device. It only pop up notification of violation.

Types of Connector:-

There are two type of Connector. First one is Smart Connector and second one is Flex Connector.

Smart Connector- These Connectors are the standard Connectors released by ArcSight for supported devices. Smart Connectors have 500+ type of supported devices of different vendor's. We can check this supported device in the list named "ArcSight Supported product list" released by ArcSight.

Flex Connector- Flex Connector is customized Connector where we have to create our own parser for the unsupported device with ArcSight. We can develop it in REGEX (Regular Expression) or in XML.

Another way is to raise F.R.(Feature Request) to ArcSight support team to create the connector for particular device.

Log Format:-

There are two types of Log format. First one is Windows Log Format and second one is Syslog Format.

Windows Log Format- Logs generated by windows System or Windows Server. For windows devices, Connector will login and uses **Pull Mechanism** to fetch the logs because windows devices do not send logs by itself.

Syslog Format- Linux, Unix or IOS systems and servers or devices which are hosted on these platform will support Syslog format and work on **Push Mechanism**. In that case, we have to configure IP address and port no of Connector on the syslog device and it will start forwarding the logs to the Connector.

How to Integrate Windows Device to ArcSight:-

In order to receive the Log on SIEM, doing the required configuration on the device end as well as on the SIEM end, is called **device integration/ data source or device on boarding**.

We can install windows connector for integrating windows-based device.

There are two types of Windows Connector

1. Microsoft Windows Event Log- Unified
2. Microsoft Windows Event Log- Native

The major differences between these connectors are-

- Performance wise Microsoft Windows Event Log-Unified Connector is better than Microsoft Windows Event Log-Native Connector.
- Unified Connector can be installed on both platform Windows OS as well as Linux OS while Native Connector can be install on Windows platform only.
- We can't modify the parser file in Windows Unified Connector while we can modify the parser file to an extend in Native Windows Connector.
- Approx. 95% of the devices can be integrated with Microsoft Windows Event Log-Unified Connector.

Steps to Windows Device Integration-

Step1:

First of all, we need to find out all devices we are going to integrate with ArcSight SIEM using the Device Inventory Document with all details i.e.: device locations.

Step2:

We have to install Windows Connector.

Only one setup file is available from the Microfocus for all the connectors. Download the ArcSight setup and install, then select the appropriate connector specific to the end device.

Step3:

Enable the connectivity between the Connector Server and the End Windows Devices. We can check the connectivity by ping command.

Step4:

Port Number SMB 445 (TCP), Should be enabled. Then only windows connectors can pull the logs.

Step5:

Required Service account with non-expiry password of each and every windows server and it should have at least read only access to the event viewer so that Connector can login and pull the log.

Step6:

Audit should be enabled on the end windows systems so that it can generate the logs and record it to the event viewer.

Step7:

Remote Procedure Call (RPC) service should be running on the end windows devices that we want to integrate. So that the Connector can pull the log from devices.

Step8:

Launch the connector that you installed and enter the IP Address/Host Name of the security Device that needs to be connected.

Step9:

Login to the domain service account by entering user name and password.

Step10:

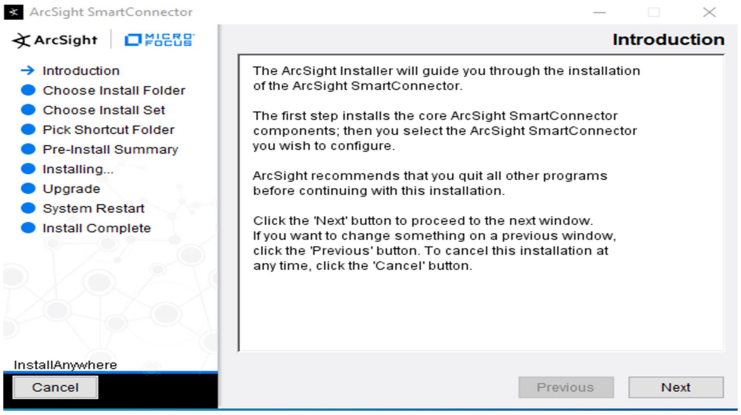
Select the OS and click on next. Once we click on the next it will check the parameters, like whether (TCP - SMB port number 445 is open or not in firewall, RPC service is enabled in end device or not and Audit is enabled or not in end device). If any parameter is not valid the it will generate the error "Parameter Validation Failed".

Step 11:

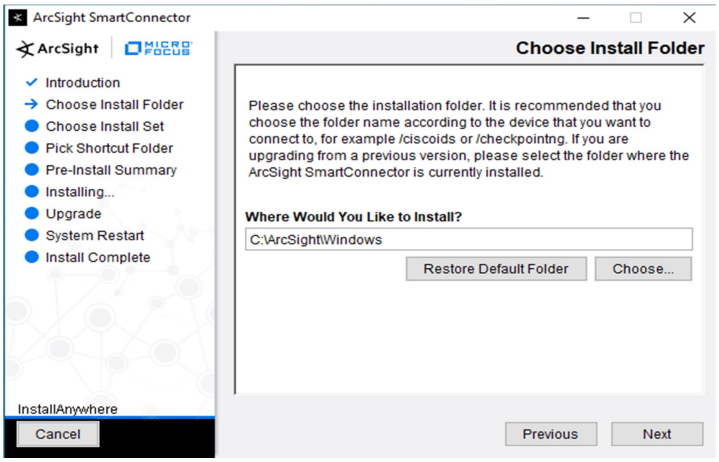
Finally, In order to verify whether devices are sending logs or not For that, Login into ESM and Logger, then give the query-"**Device Address= <IP Address of the End Device>**"

Windows Connector Installation Step by Step:-

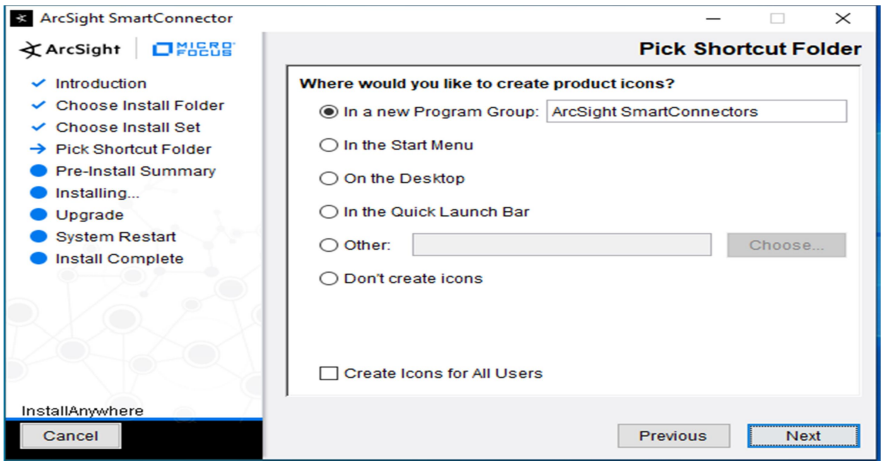
1- Launch the connector setup file as "**Run as administrator**".

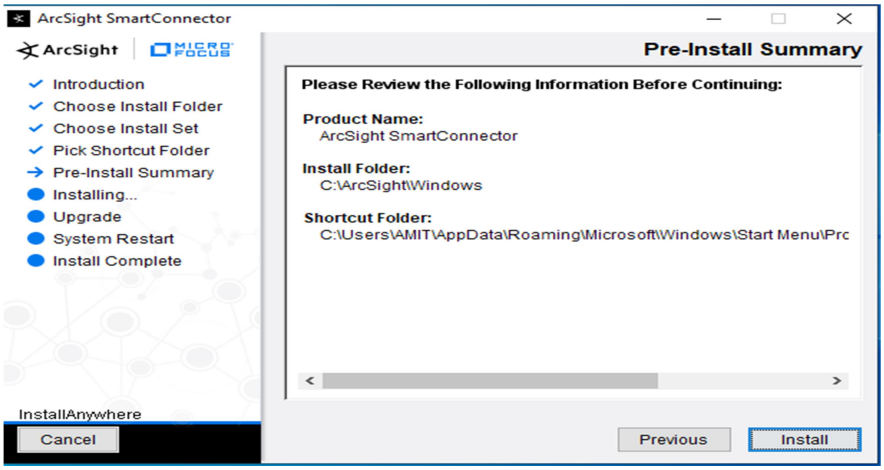


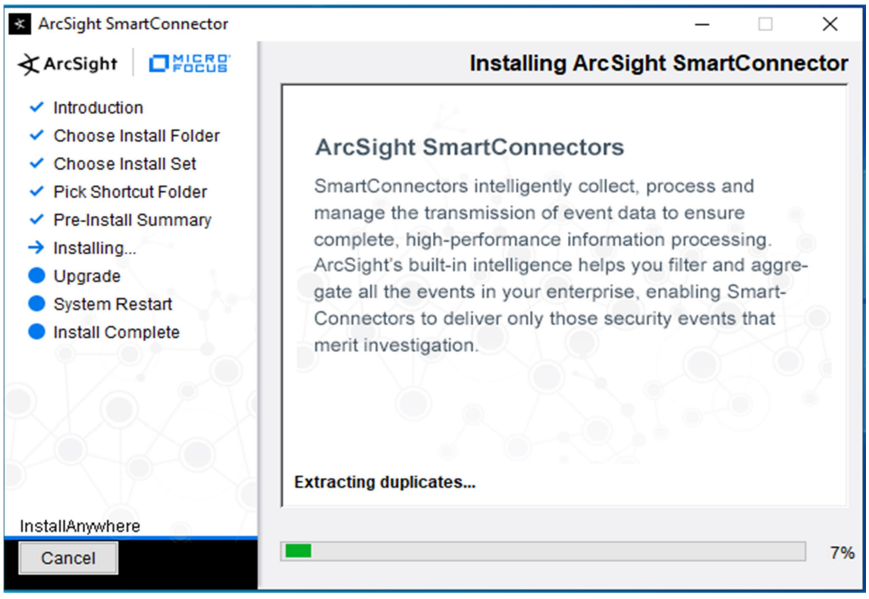
2- Select the path where we want to install the connector.



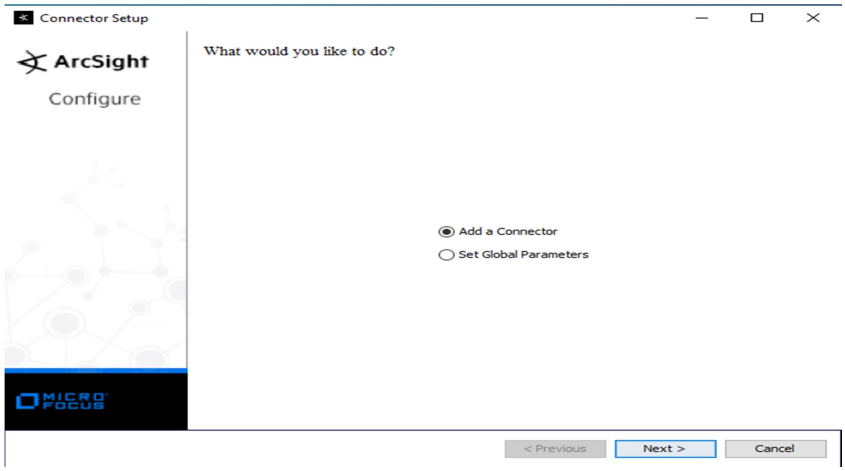
3- Keep as default below and select **Next** and then **Install**.



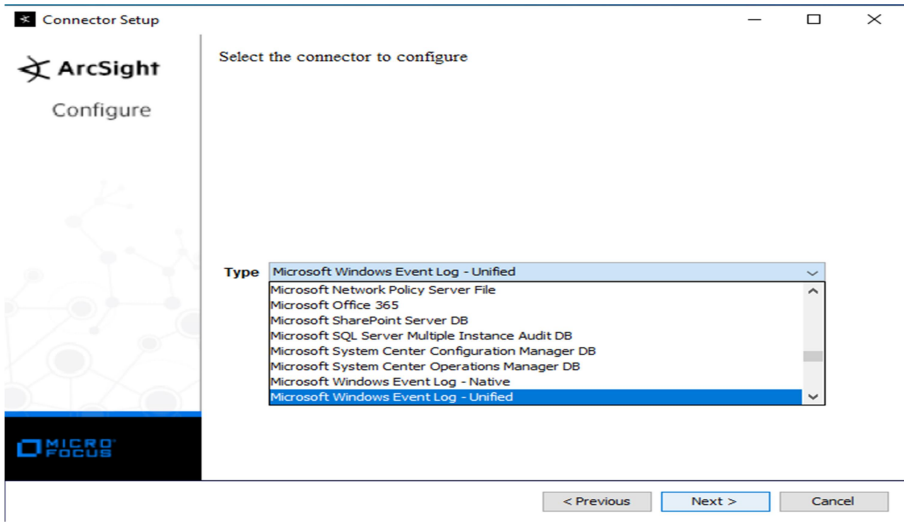




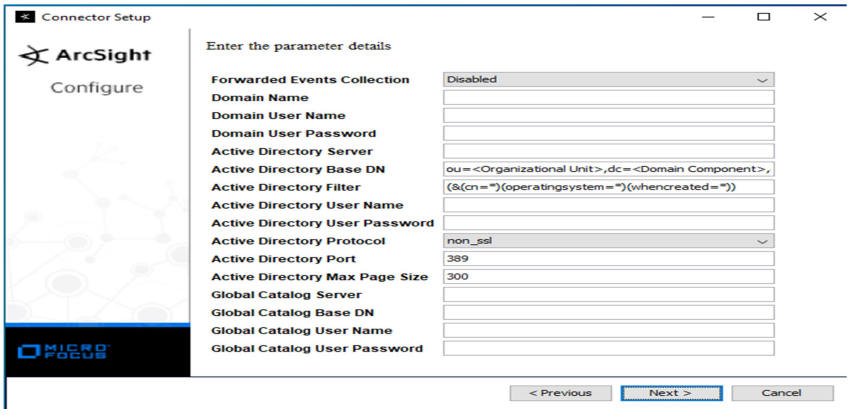
4- Select "**Add a Connector**".



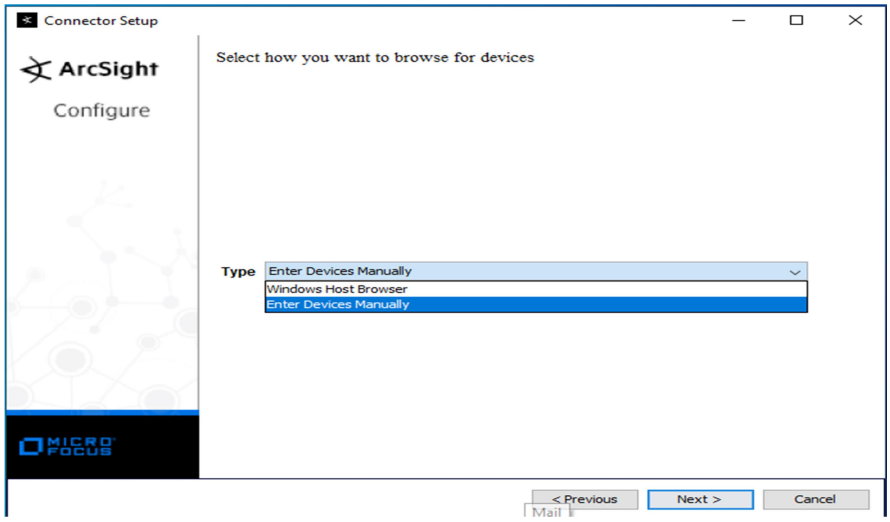
Select Type as "**Microsoft Windows Event Log-Unified**".



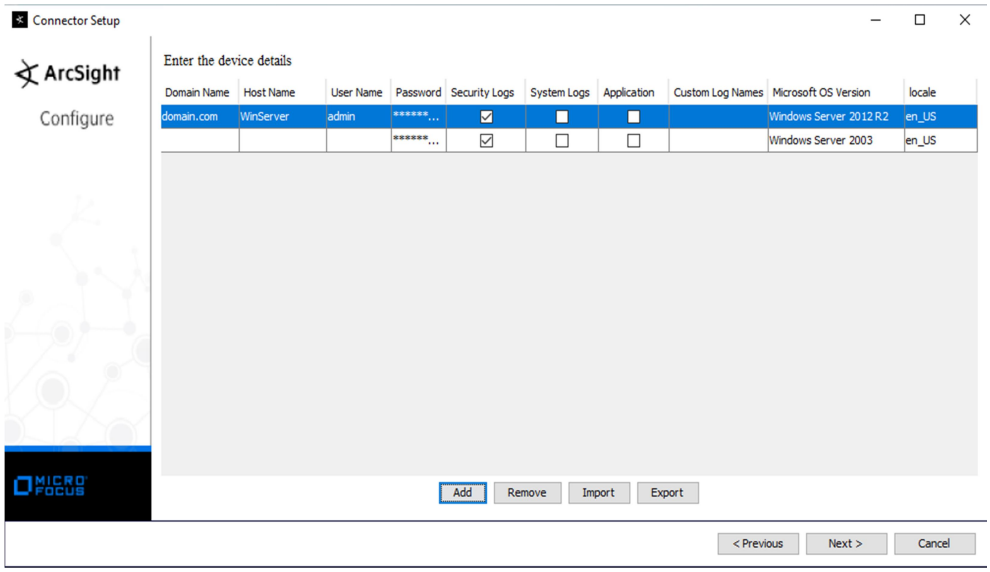
5- Leave default as below.

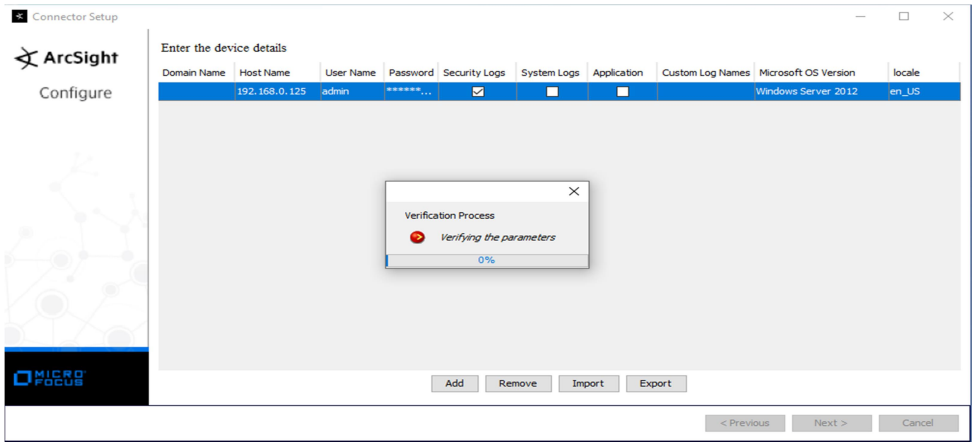


6- Select "Enter Device Manually"

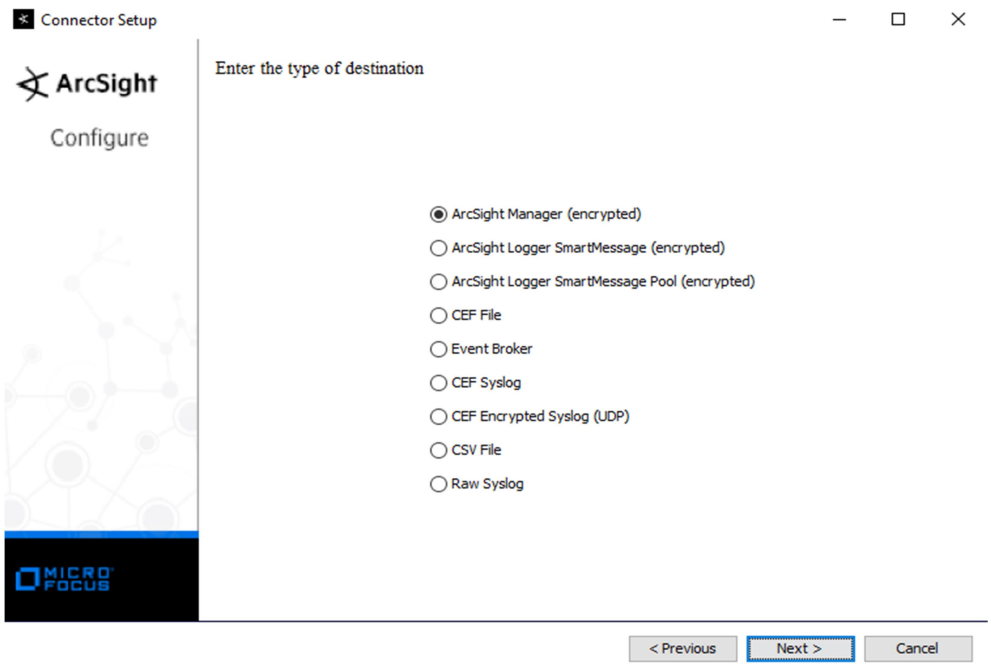


7- Enter device details then **Next**.

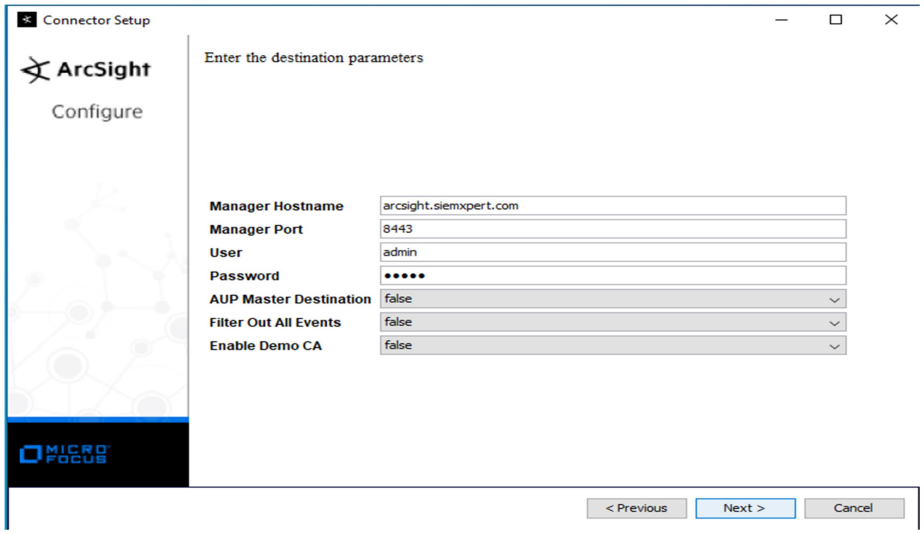




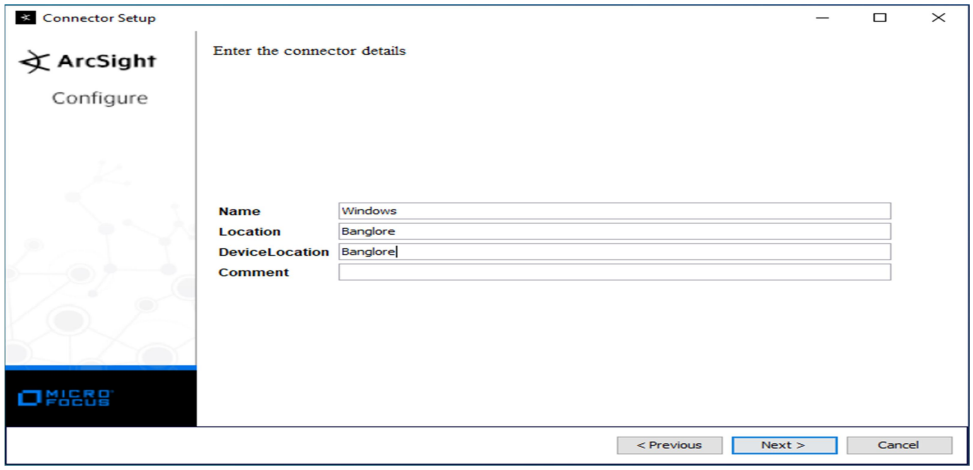
8- Select destination as "**ArcSight Manager{Encrypted)"** or "**ArcSight Logger SmartMessage(Encrypted)"** as per requirement.



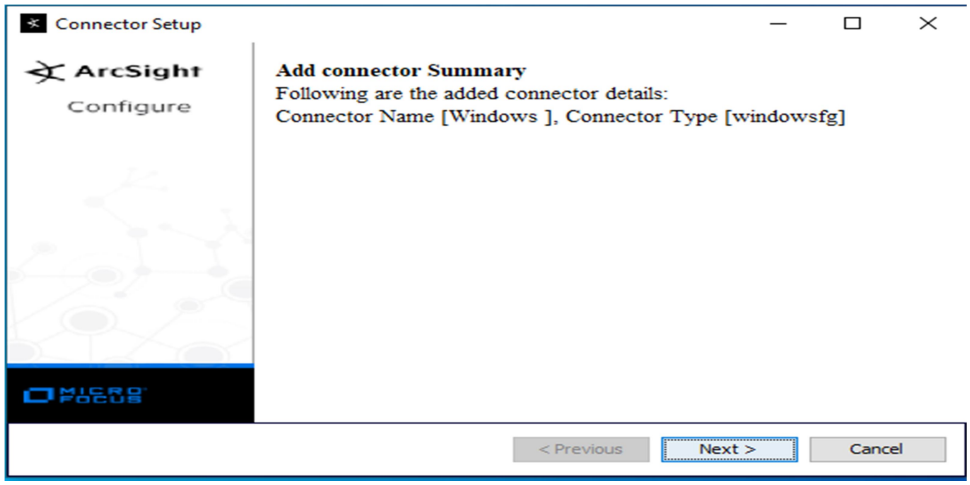
9- Enter ESM Manager details. ie: hostname, user and password.



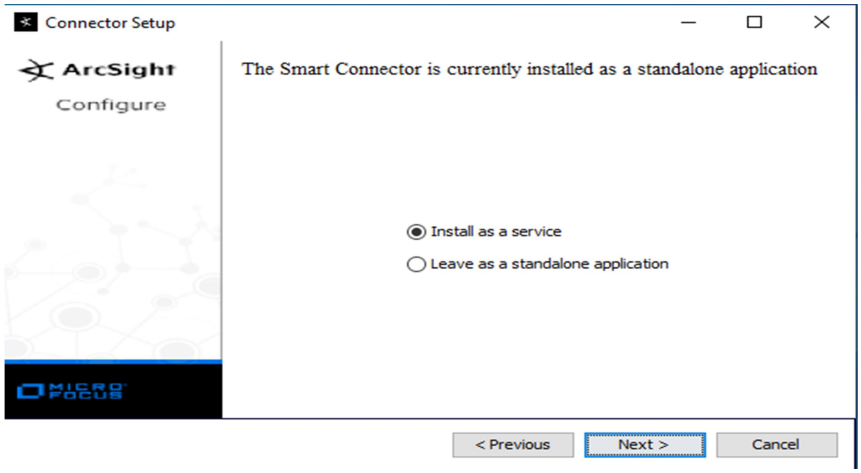
10- Enter Connector information.



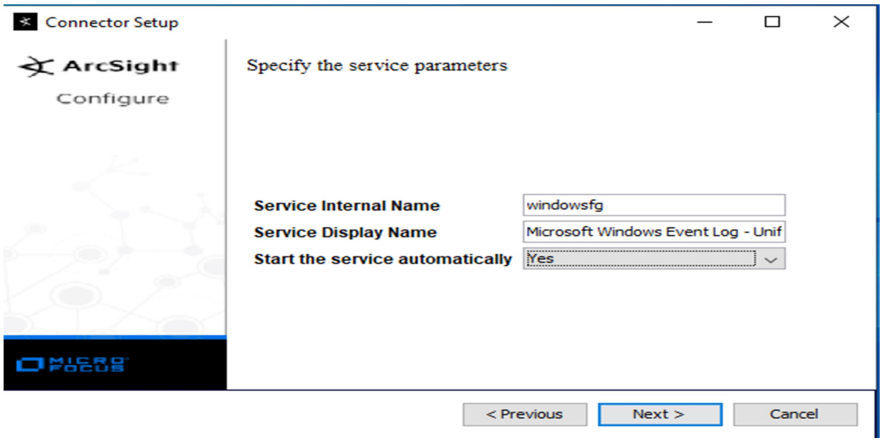
Will receive summary like below.



11- Select "**Install as a Service**".

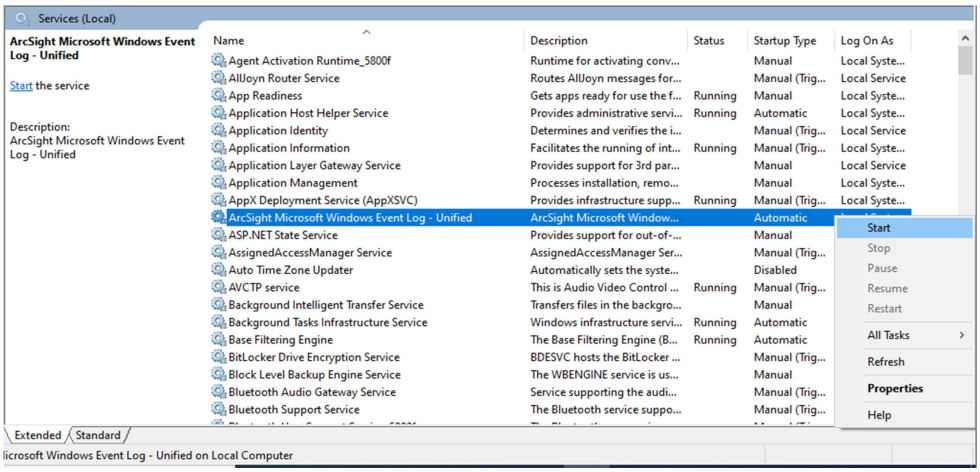


Specify the parameters as below then **Next** and then **Exit**.



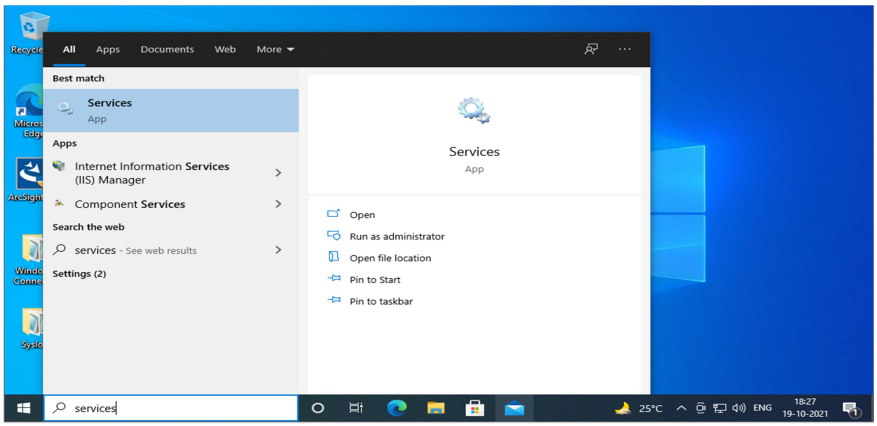
Connector is installed successfully.

12- Now Check weather service is start or not. If not then start as below.

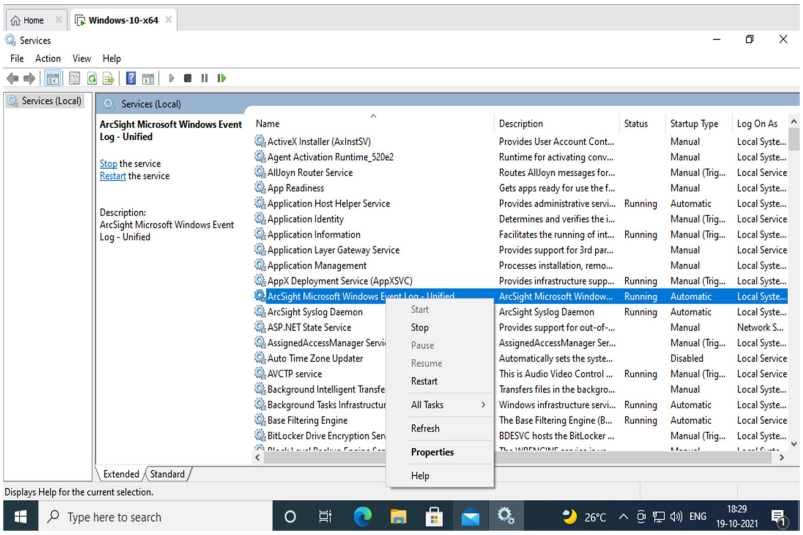


Windows Connector Uninstallation Step by Step:-

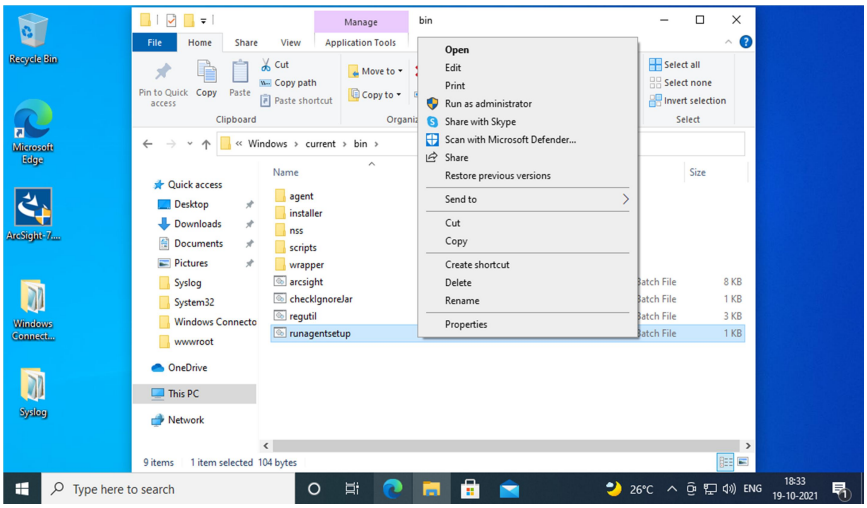
1. Stop the Connector Service by navigating
Search box -> type **Services** -> Click on Services



Select service **ArcSight Microsoft Windows Event Log – Unified -> right click** -> click **Stop** to stop running service.

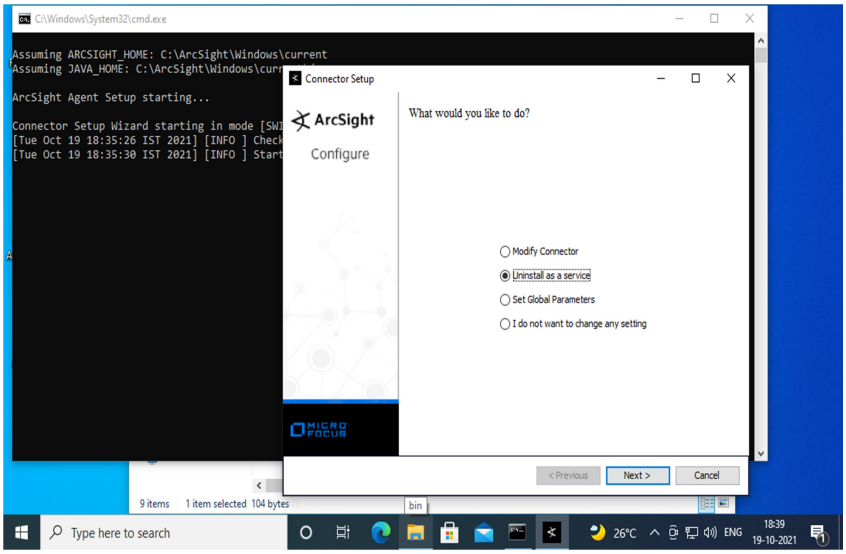


2. Browse connector folder where it is installed ie: **C:\ drive -> current -> bin** -> right click on **runagentsetup** batch file -> select **Run as administrator**.

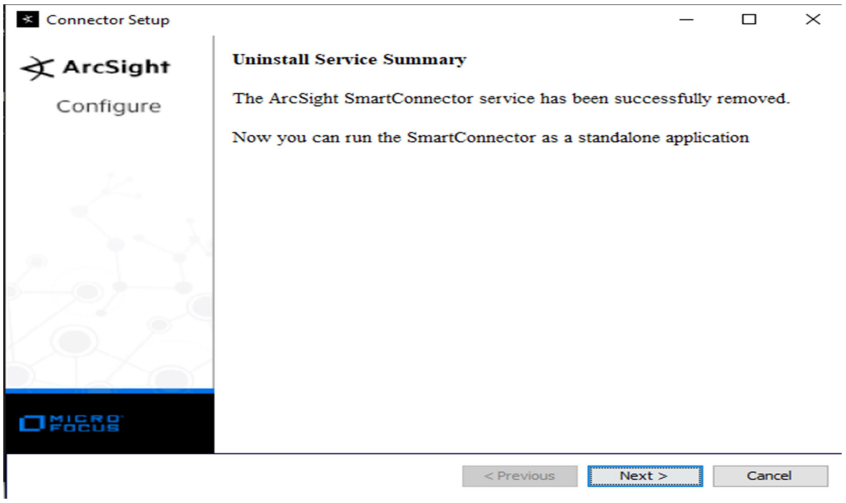


Here **ArcSight Agent Setup** window will appear.

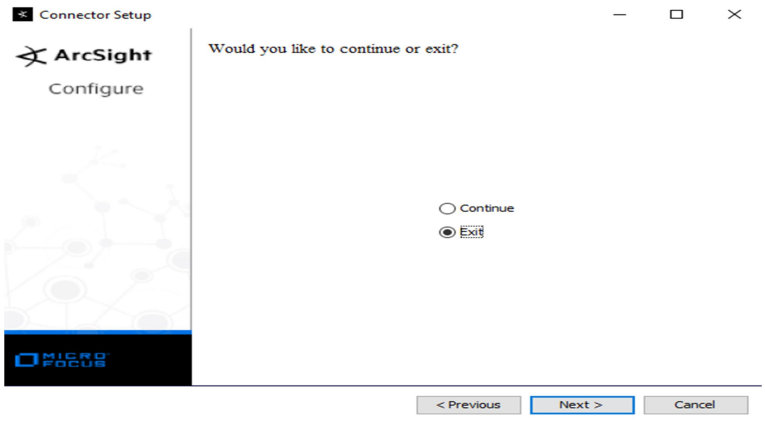
Now select **Uninstall as a service** -> **Next**



Uninstall as a service is mandatory to remove services before connector uninstallation skip getting error while reinstallation. Here, we will get successfully Uninstallation message of ArcSight connector service.



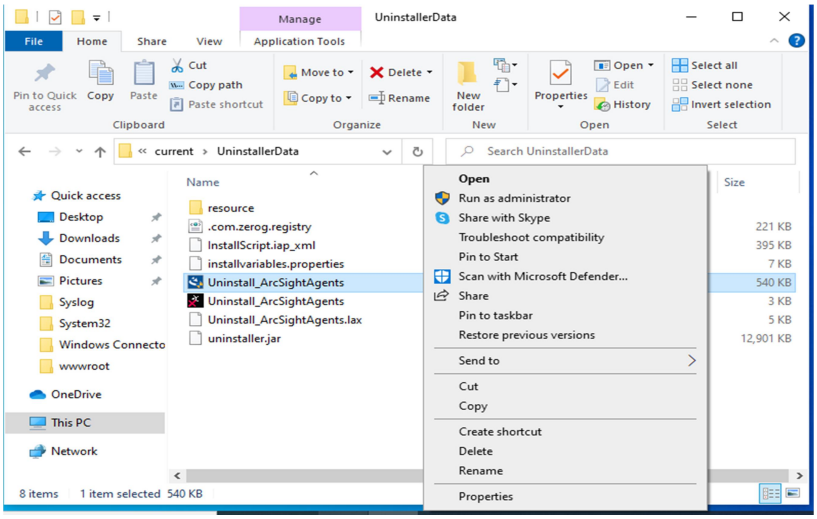
Click on **Next**

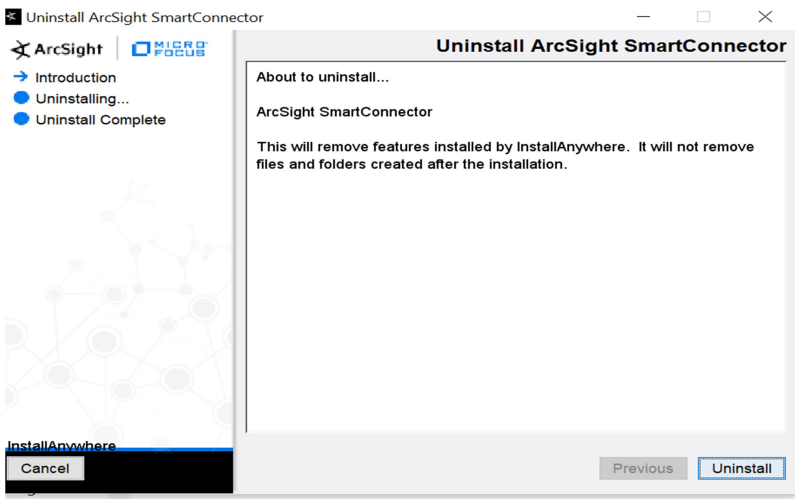


Finally click on **Exit-> Next**

3. Now verify that connector service is removed and does not exist anymore in Windows Services.

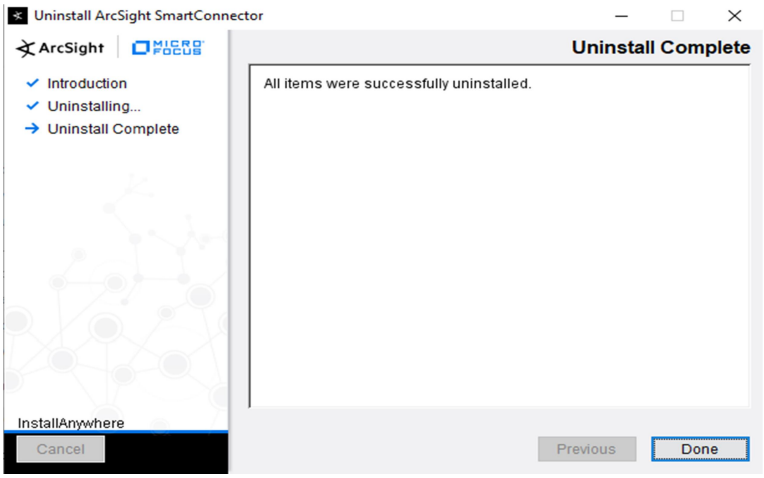
4. Browse connector folder where it is installed -> **current -> current -> UninstallerData** -> right click **on Uninstall_ArcSightAgents** application file -> select **Run as administrator.**



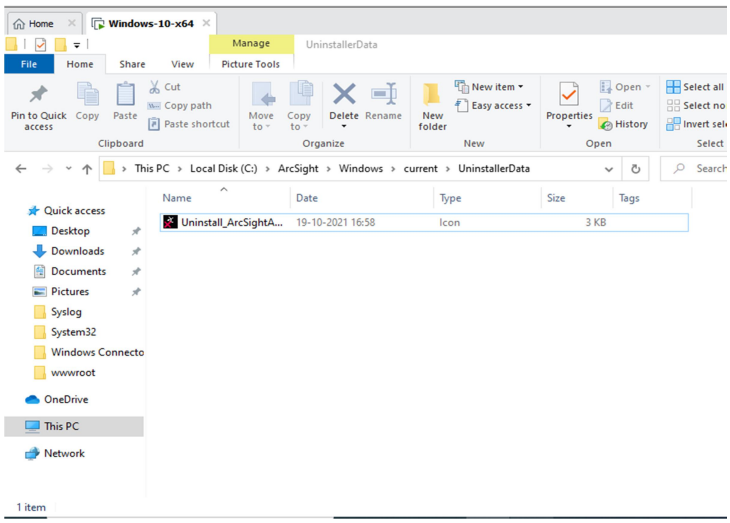


Select **Uninstall-> Done**

We will get successfully Uninstallation message of ArcSight connector.



Also all the files & folder will be deleted automatically as in below screenshot.

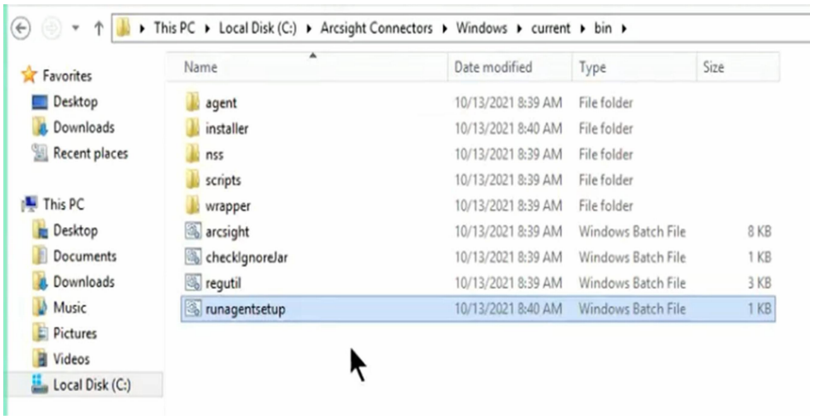


After all, we can delete residual files & folder from main folder of connector. Uninstallation of all the connector will be same like this.

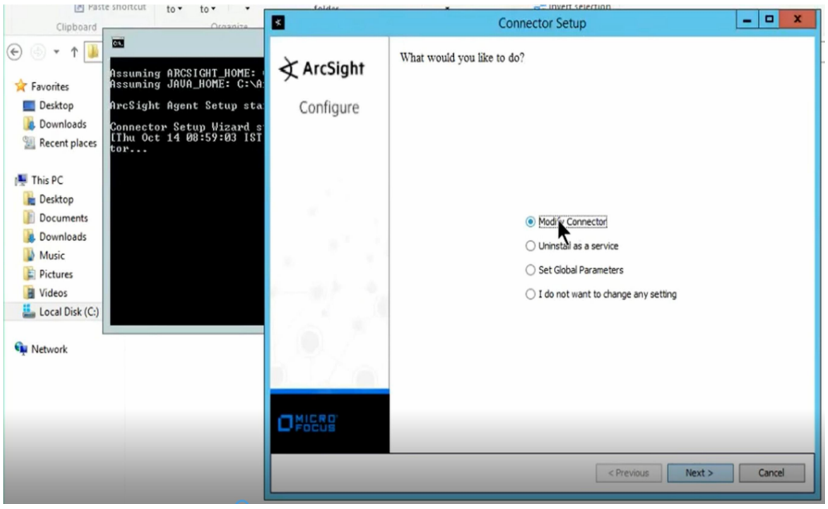
Relaunch Windows Connector to add new device Step by Step:-

1- Go to the folder where the connector gets installed (Here, C:\ArcSight Connectors) and visit below path C:\ArcSight Connectors\Windows \current\bin

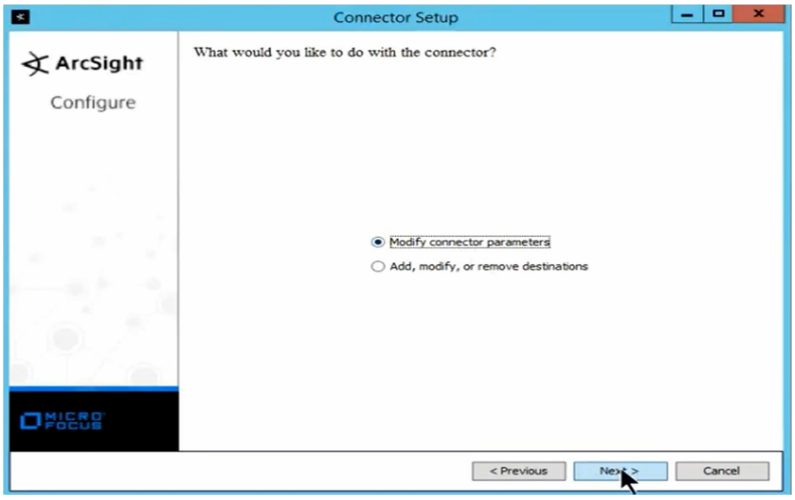
2- Choose the last setup file **(runagentsetup)** -→Right Click --→ **Runs as administrator**

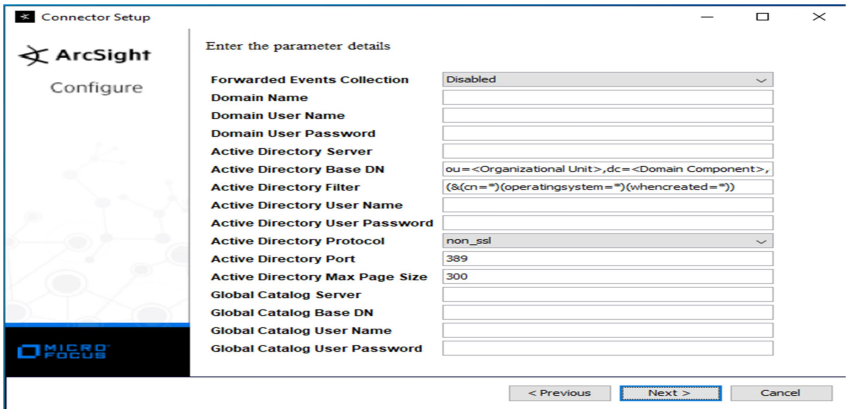


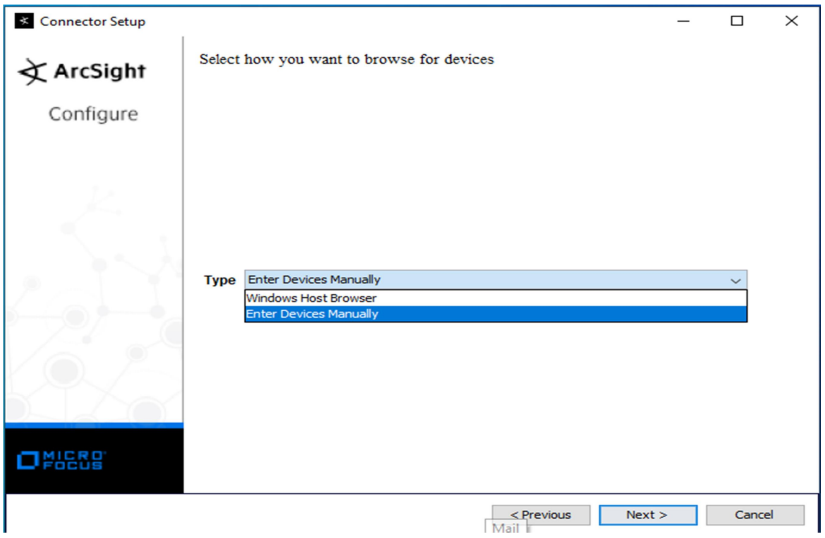
3- Select "**Modify connector**"

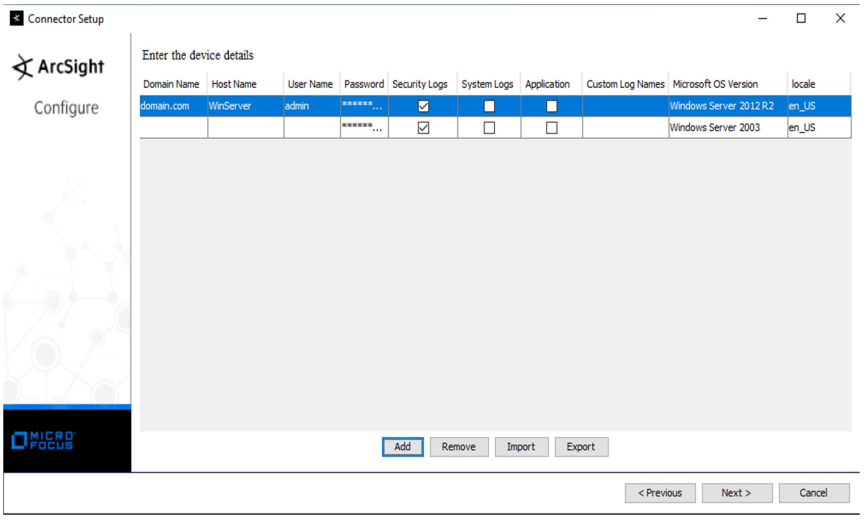


4- Select "**Modify Connector Parameters**"









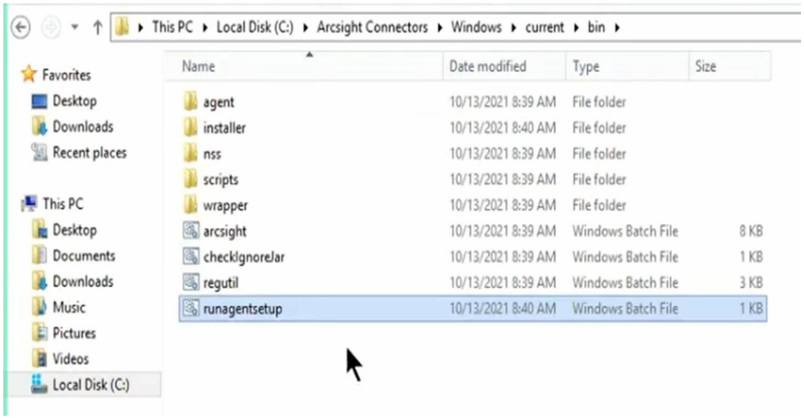
Here we can add devices.

Relaunch Windows Connector to add logger as dual destination Step by Step:-

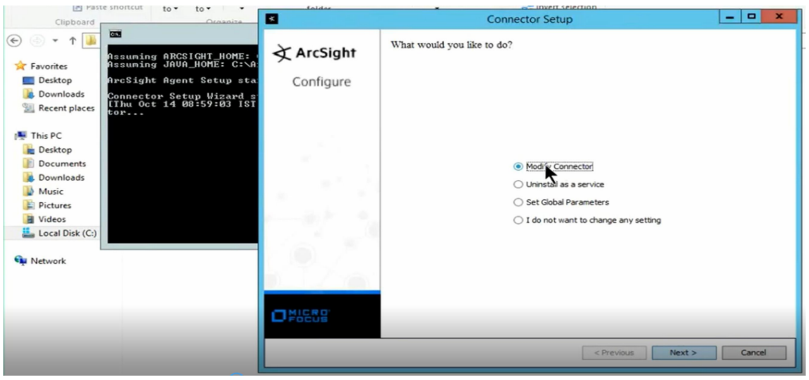
1- Go to the folder where the connector gets installed (Here, C:\ArcSight Connectors) and visit below path

C:\ArcSight Connectors\Windows \current\bin

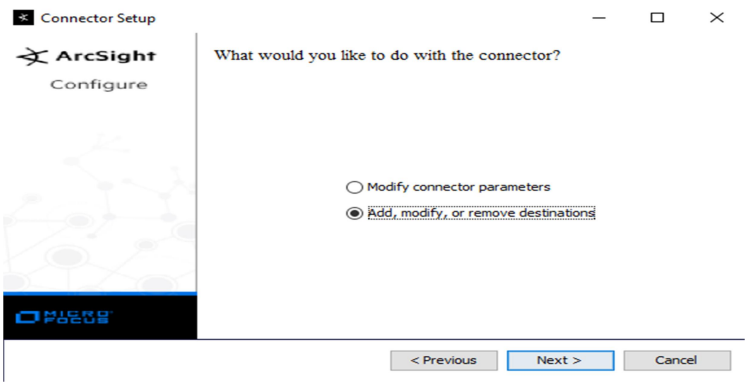
Choose the last setup file **(runagentsetup)** →Right Click → **Runs as administrator**

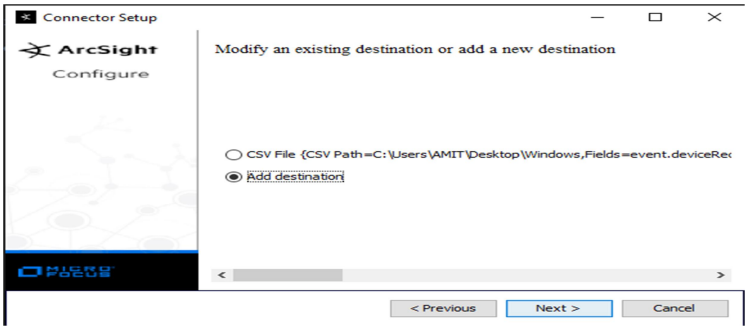


2- Select "**Modify connector**"

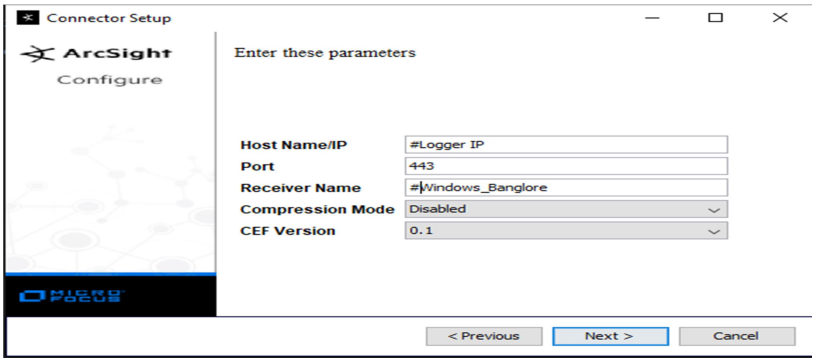


3- Select "**Add, Modify, or remove destinations**"





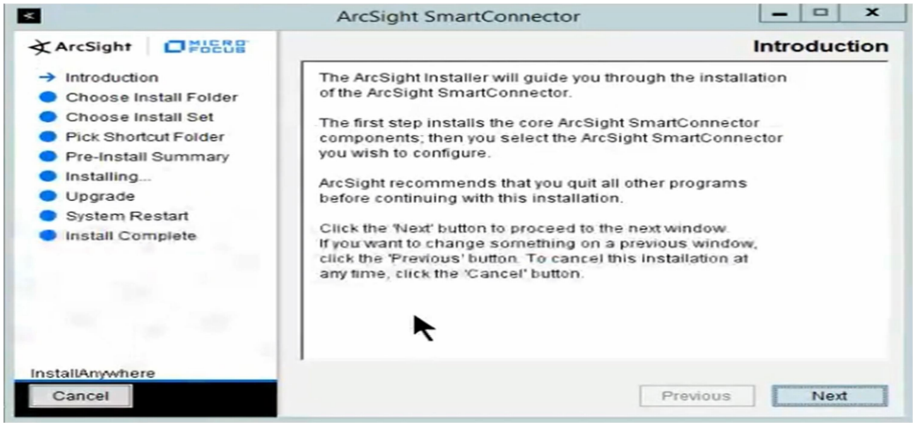
4- Enter Logger details IP and Receiver name same as mentioned in Logger.



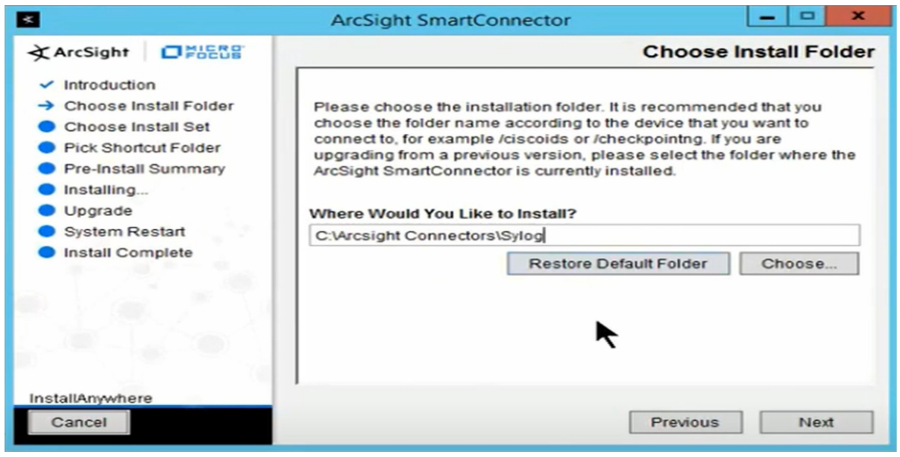
Click **Next,** Will receive summary like below.

Syslog Daemon Connector Installation Step by Step:-

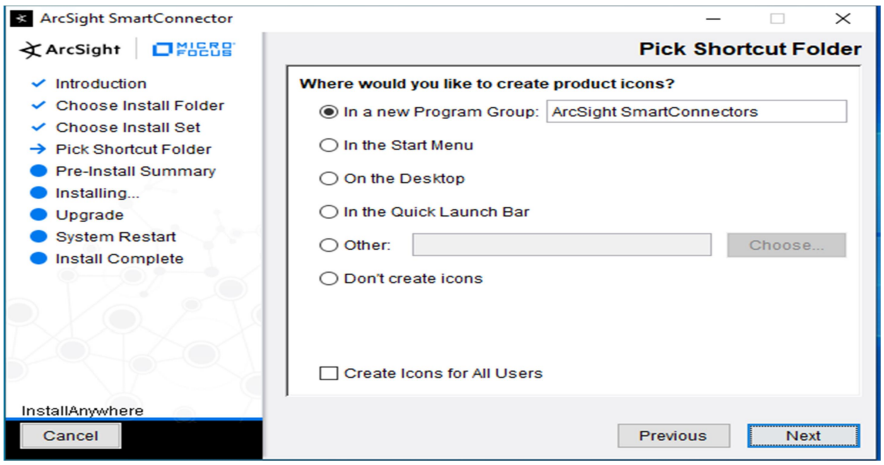
1- Launch the connector setup file as "**Run as administrator**".

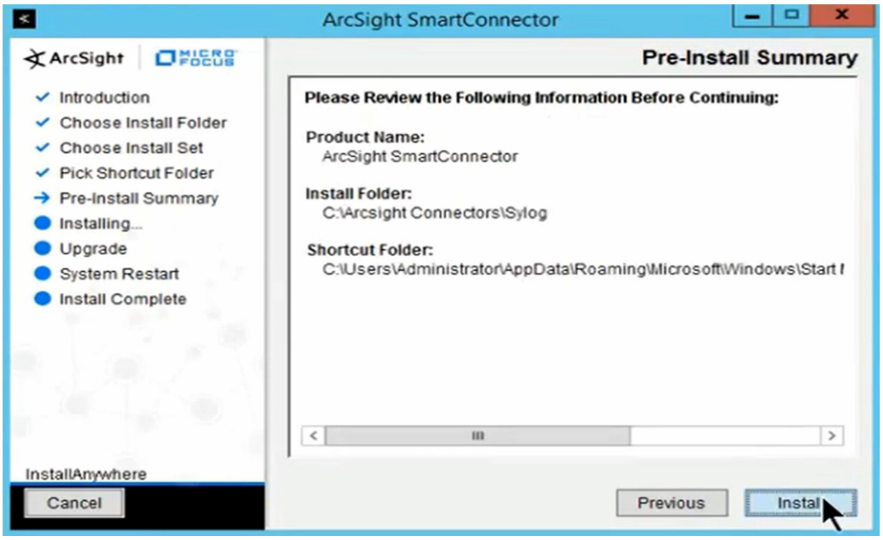


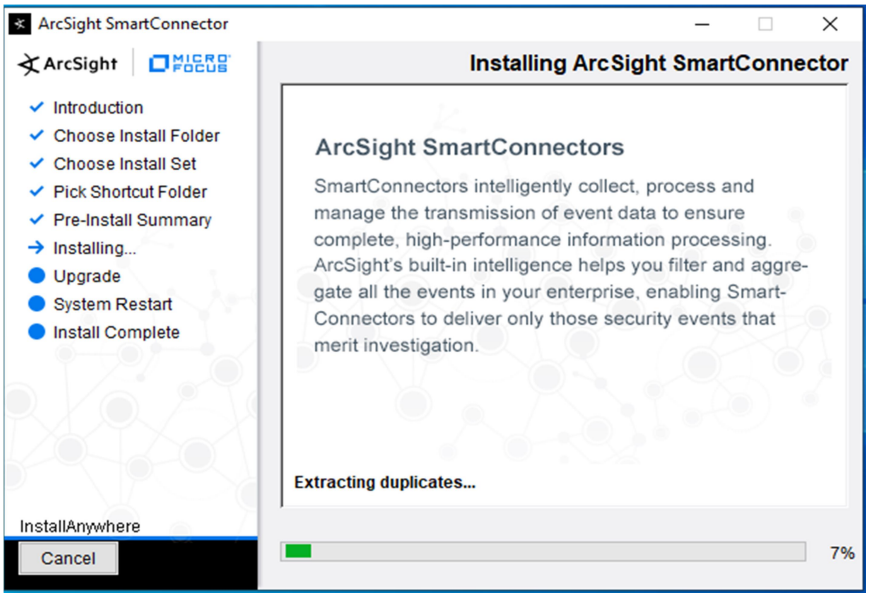
2- Select the path where we want to install the syslog connector.



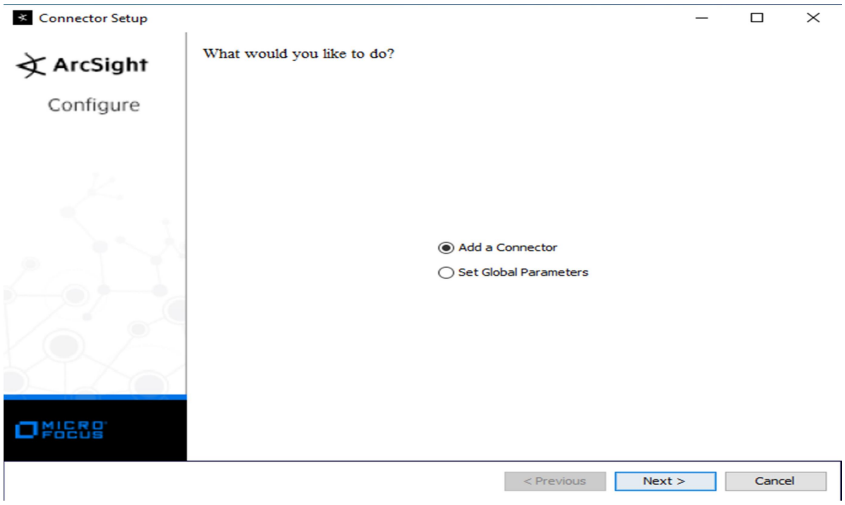
3- Keep as default below and select **Next** and then **Install**.



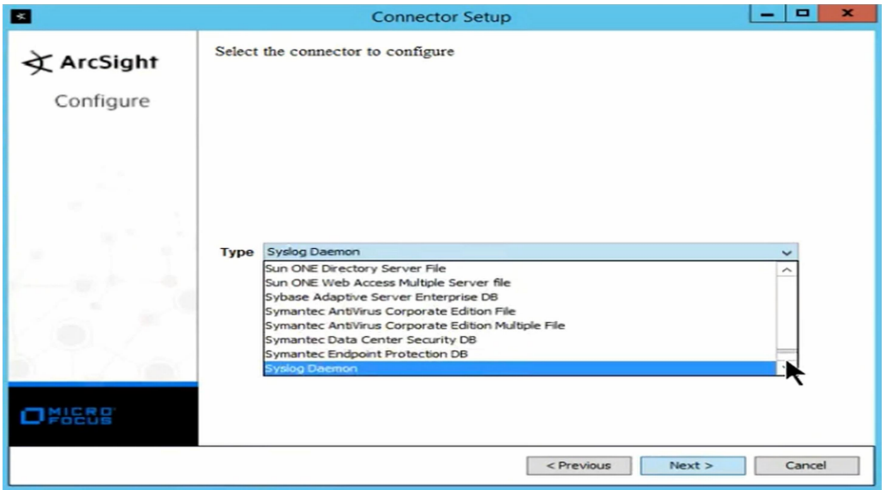




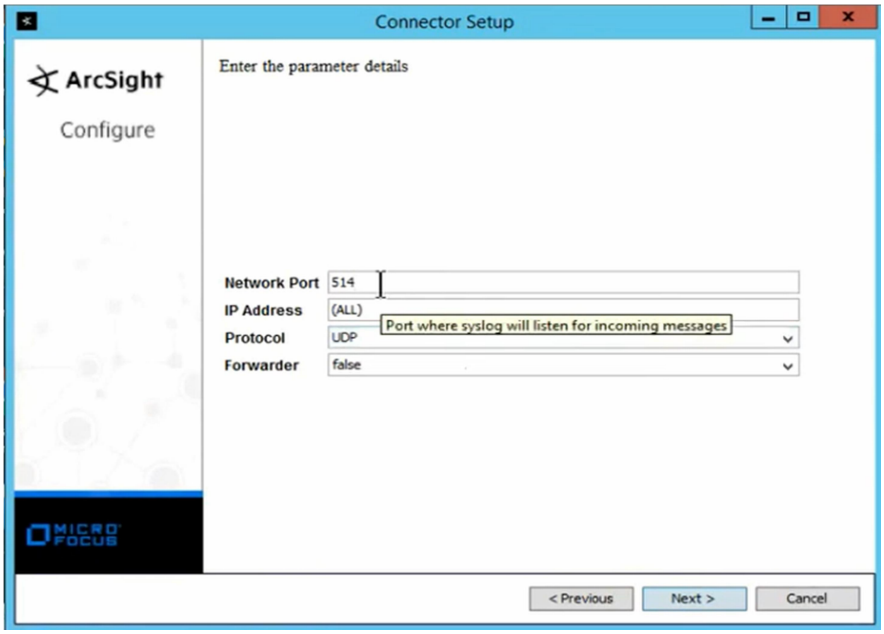
4- Select "**Add a Connector**".



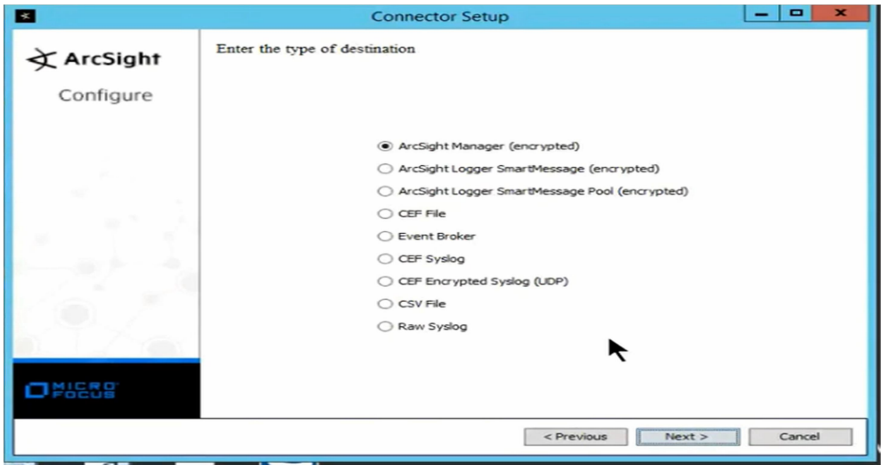
Select Type as "**Syslog Daemon**".

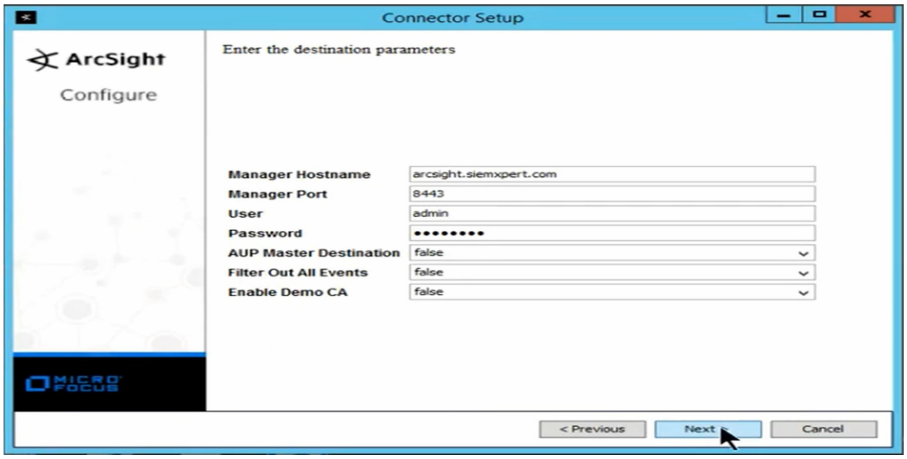


5- Fill **IP address, port no and protocol** then **Next**.

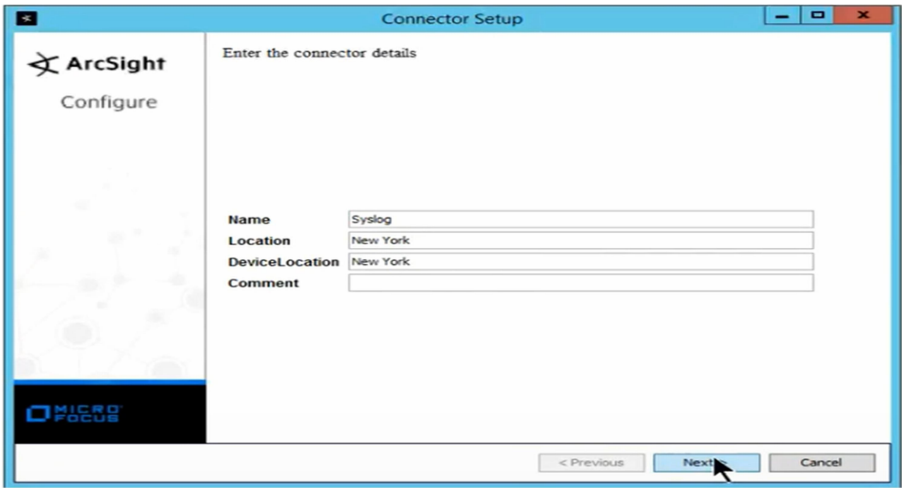


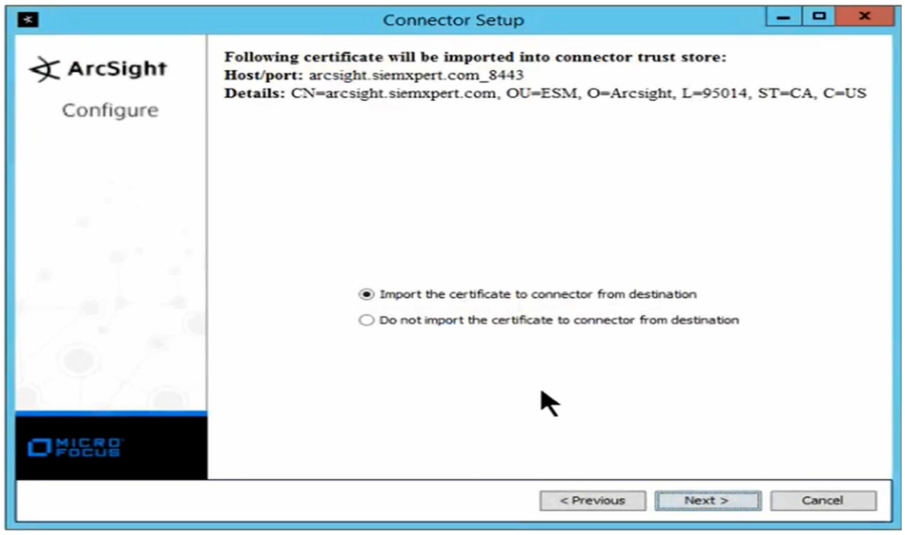
6- Select the destination where log has to be sent.

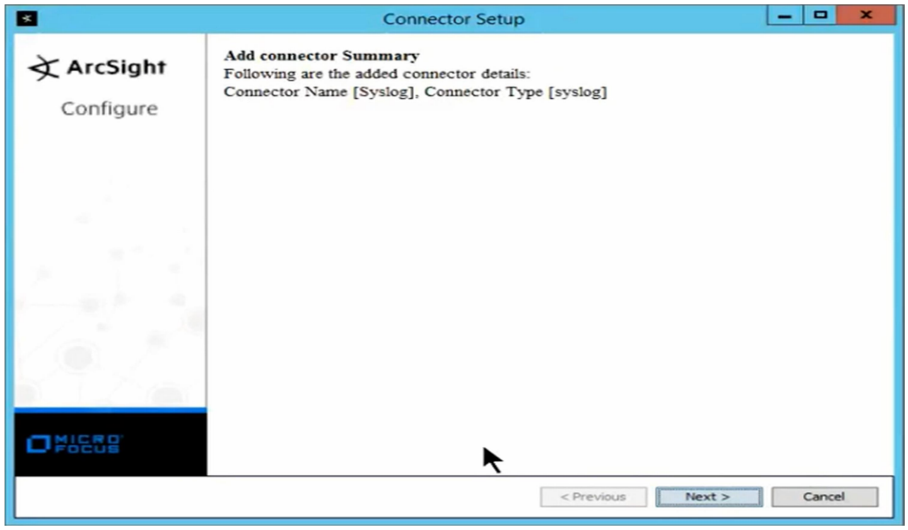




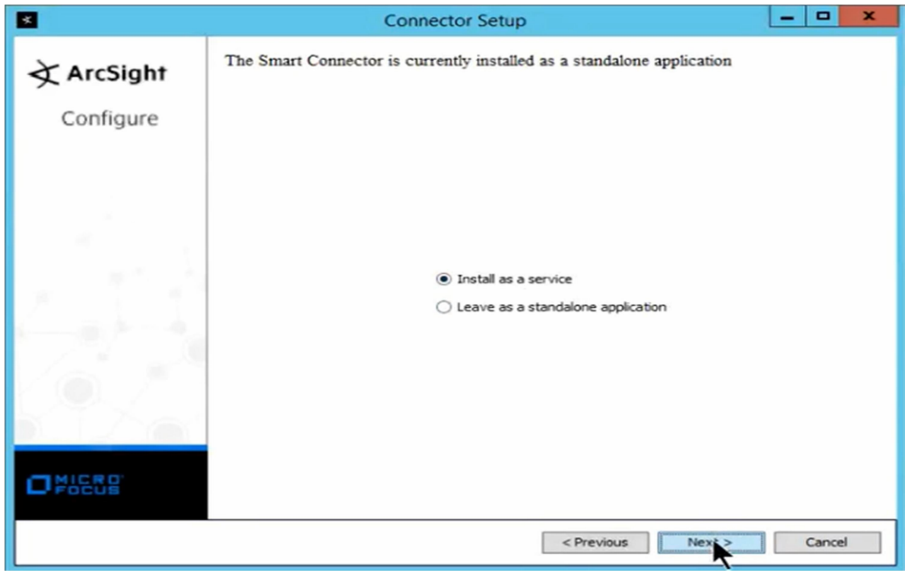
7- Enter connector details.



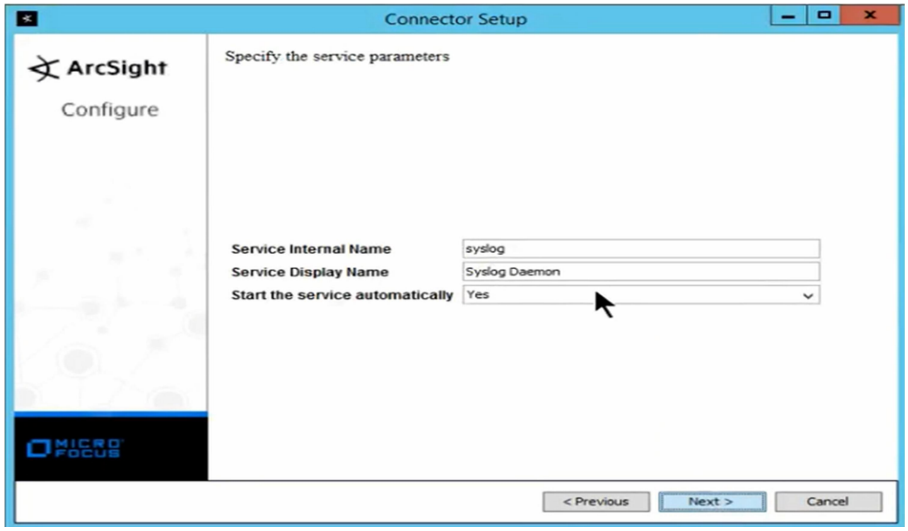


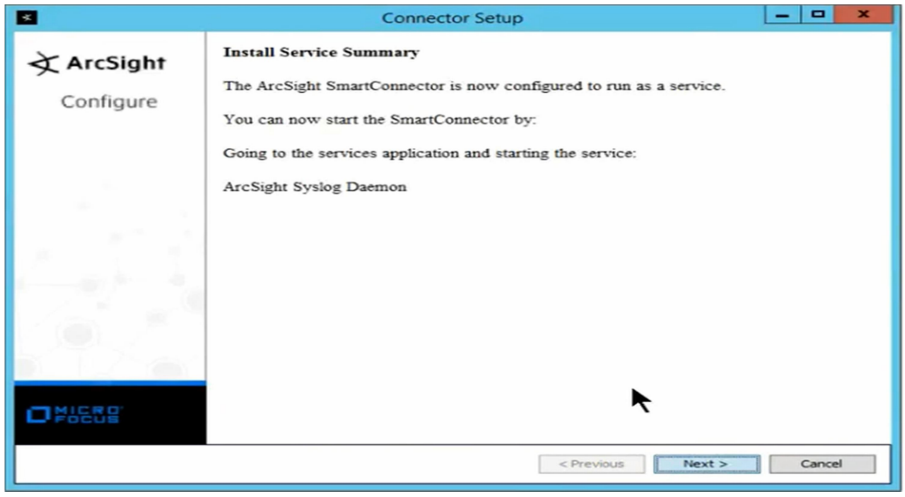


8- Select "**Install as a service**".

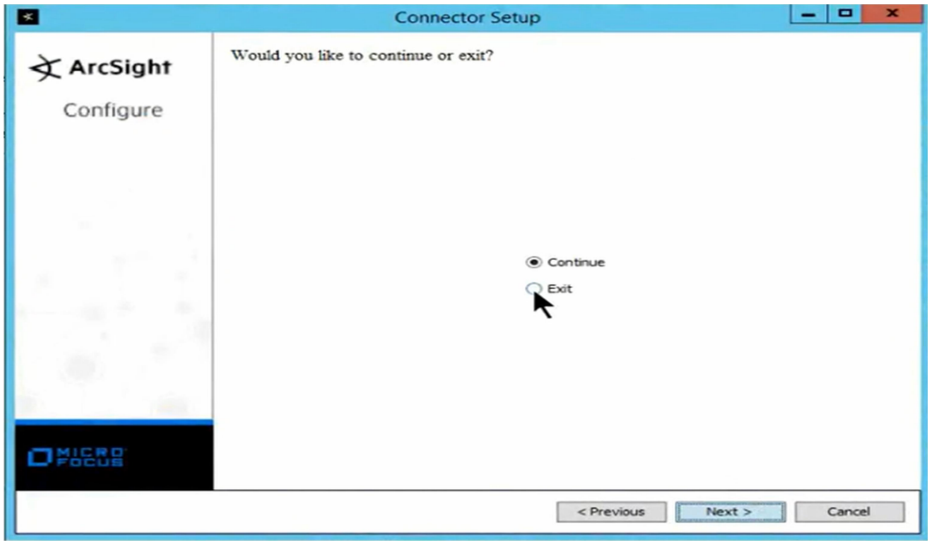


9- Specify the service perimeters as default below.

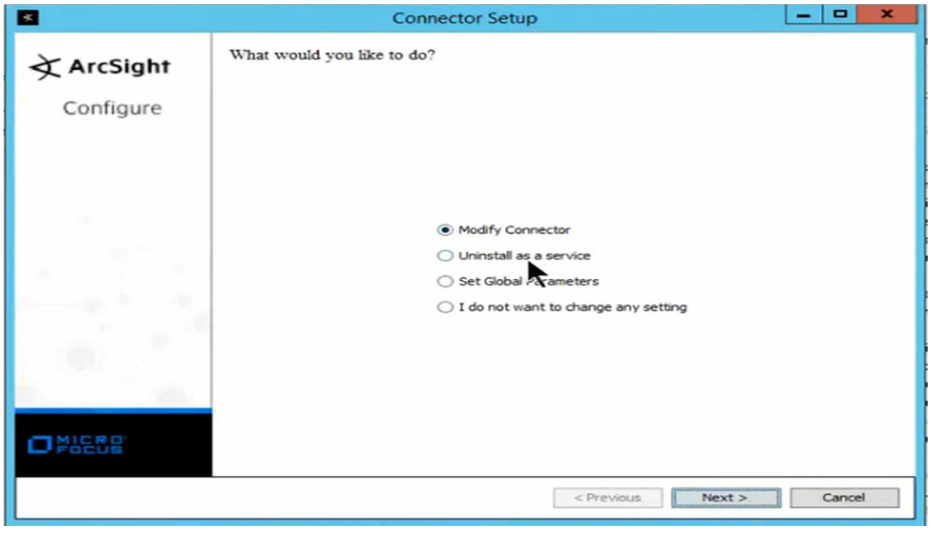




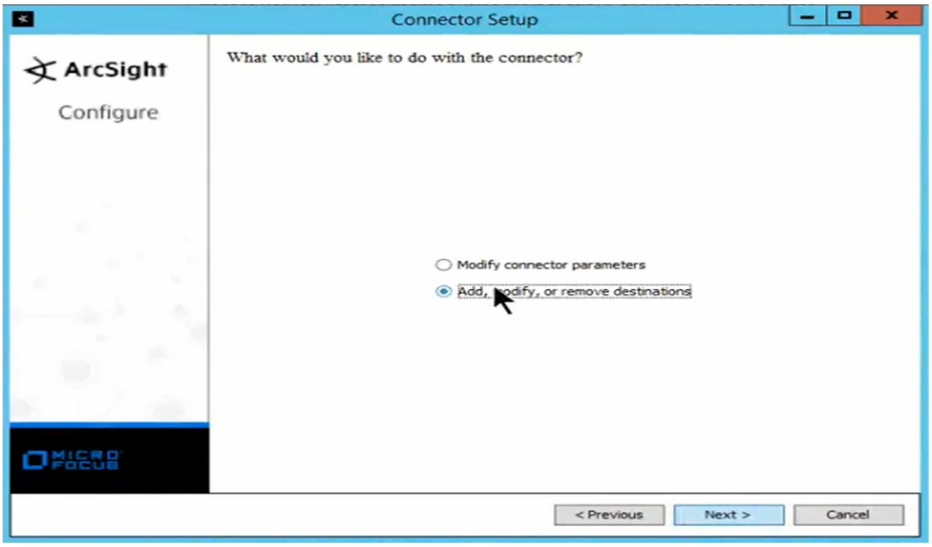
10- Click on **Continue** to select Logger also**.**



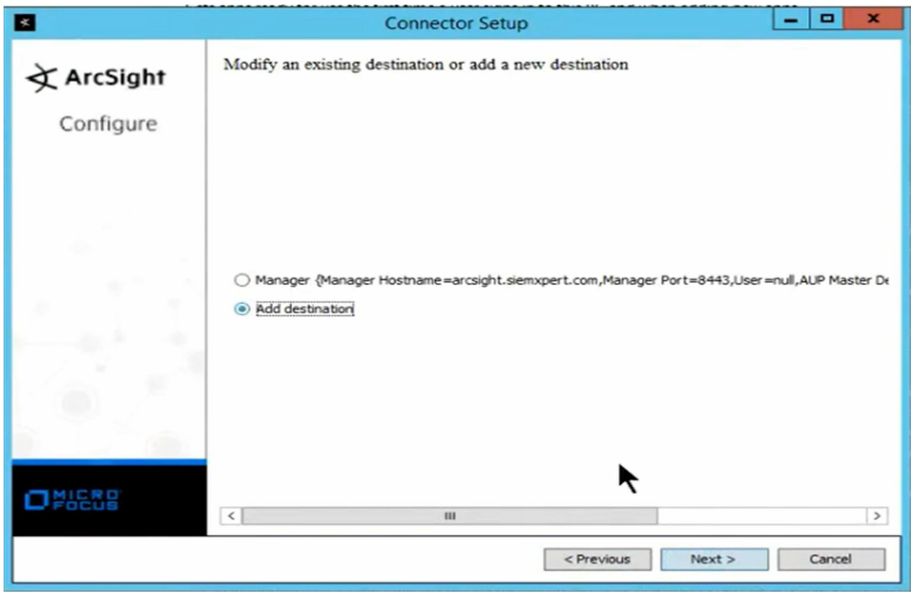
Select Modify Connector



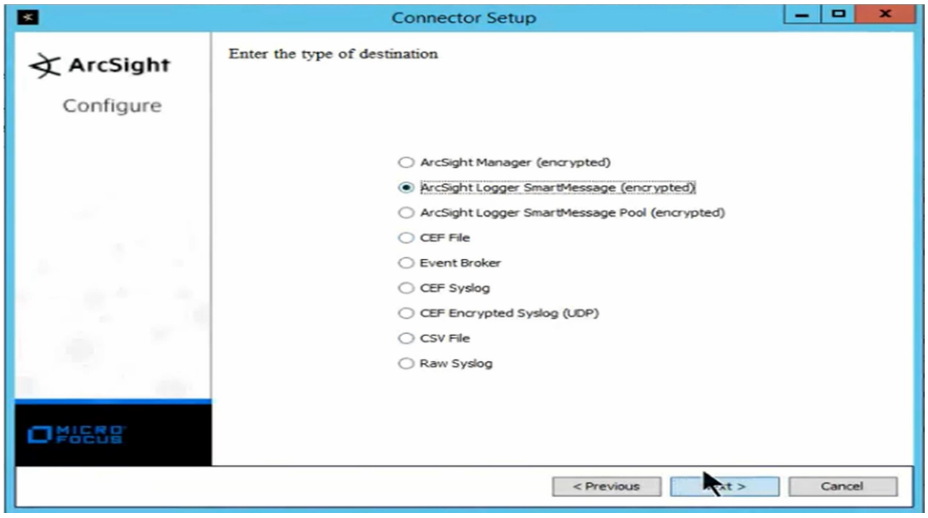
Select "**Add, modify or remove destinations".**

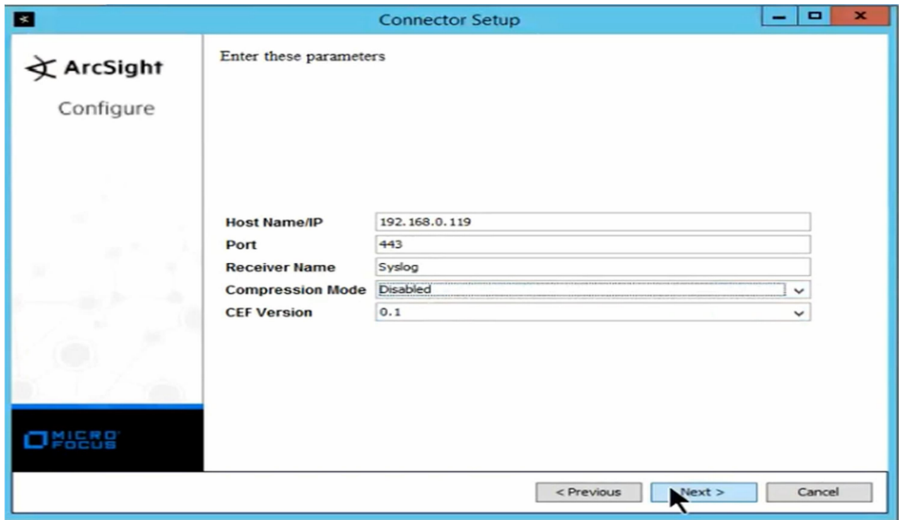


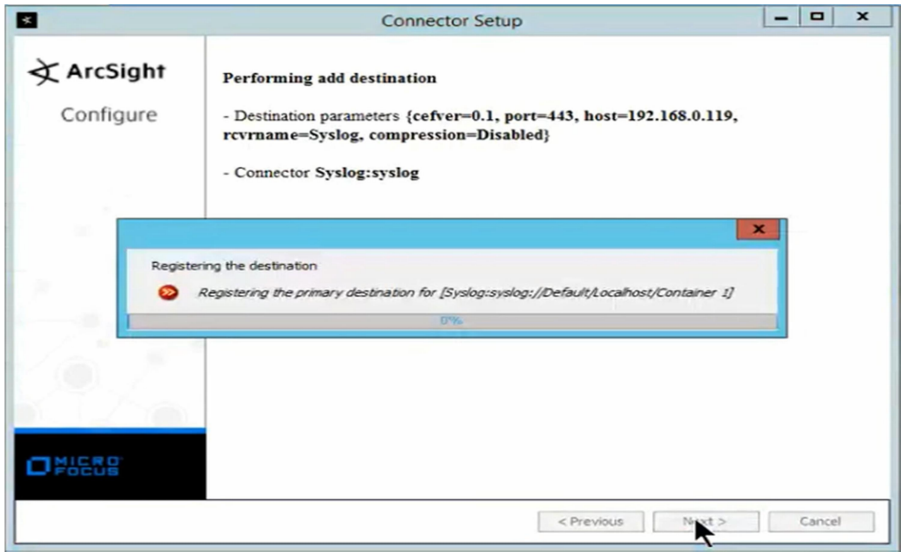
Select "**Add destination**".



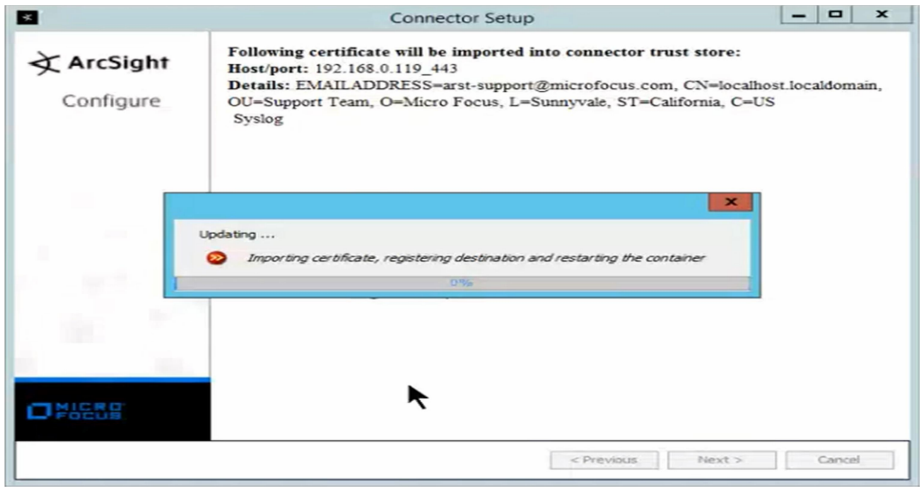
Select "**ArcSight Logger SmartMessage (encrypted)**".

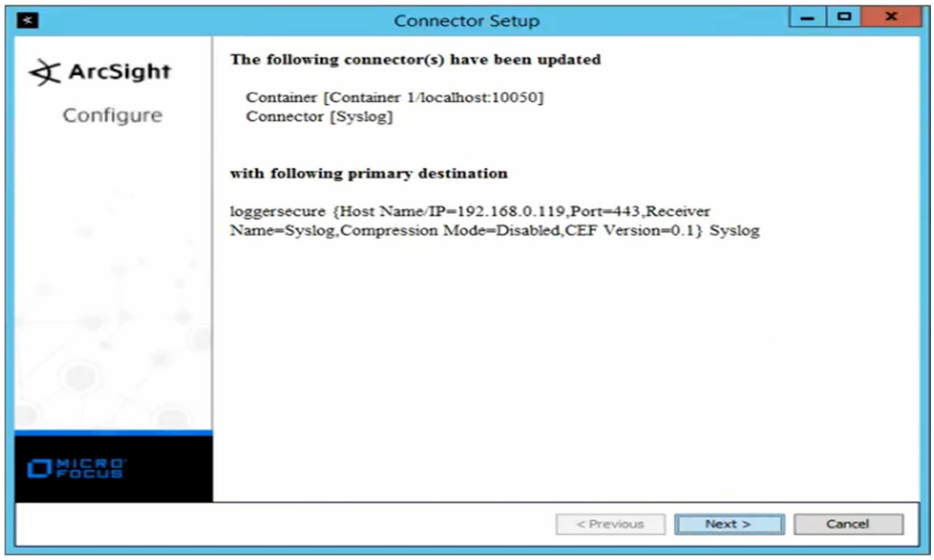


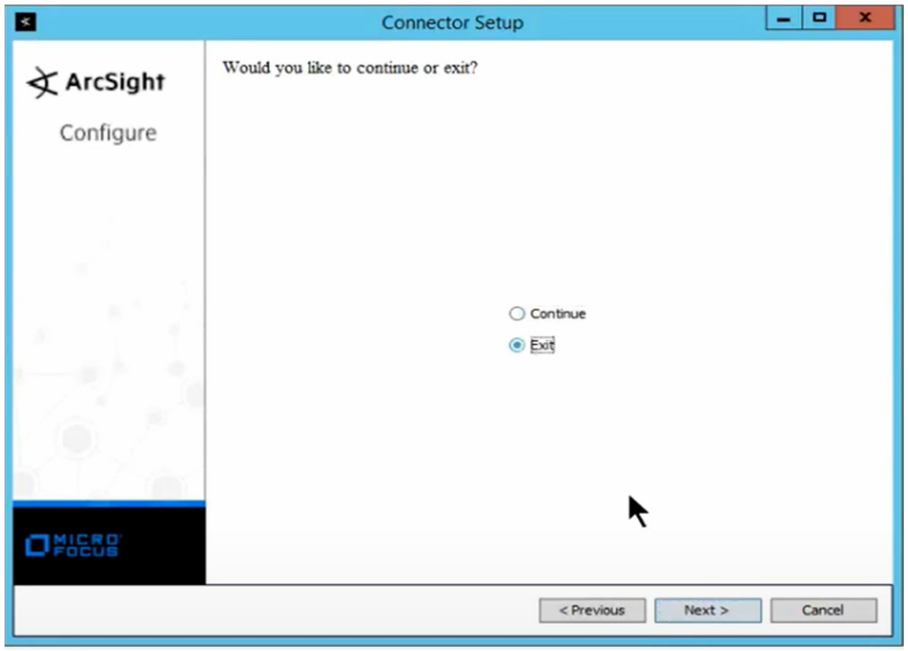




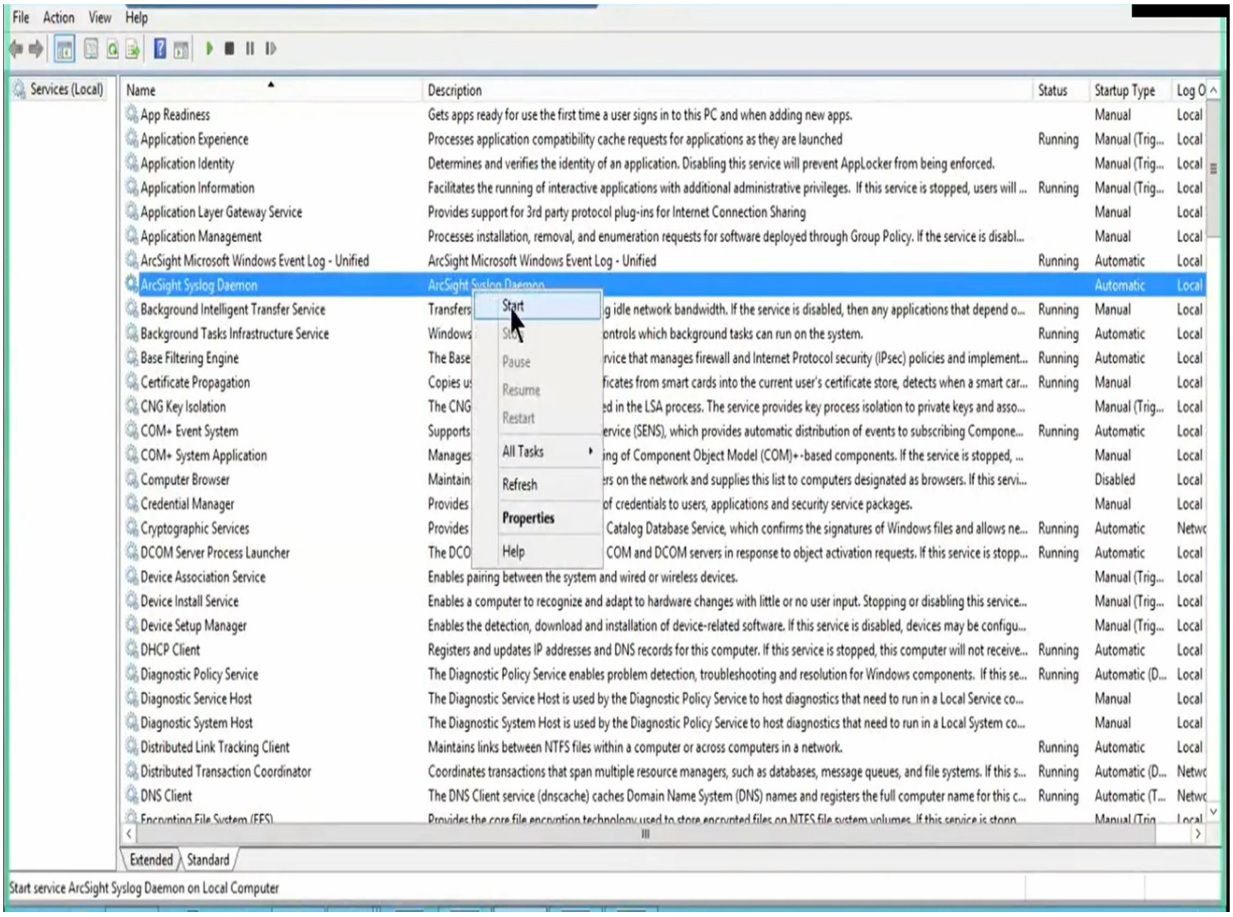
Select “Import the certificate”.







11- Start the **Syslog Daemon** service.



How to Integrate Syslog Devices to ArcSight:-

Step 1

Check in "ArcSight supported product list" of Microfocus, whether the integrating device is supported by the ArcSight or not.

Link for ArcSight supported product list document: https://www.microfocus.com/media/flyer/arcsight_connector_supported_products_flyer.pdf

Step 2

If the device is supported by the ArcSight, then download the device integration document for the specific device.

Device Integration Document will give the below information:

- Versions of devices it supports.
- Name of the Connector.
- How to install or configure connector.
- What kind of configuration has to be done on the end devices which we are going to integrate.

If the device is not supported by ArcSight then we have to go with Flex Connector.

Step 3

Install the respective Syslog connector on connector server which is mentioned in the Device Integration Document.

It can be either Default Syslog Daemon Connector or Syslog Dedicated Connector.

Then, Configure the Port number and Protocol on the Connector. So that the connector can listen the logs from the devices.

Protocol: UDP – It is unreliable

We can also use TCP, if the server can support high bandwidth. The advantage of using TCP is, it offers a guaranteed delivery of data packets (Logs). So, TCP is more reliable than UDP.

Port Number: 514 (Default Port Number), 515,516,517,518,519 Then after 1024 (since 0 – 1023 are reserved ports)

Note: If you configured port number 514 to one of the Syslog connectors on the server, then you cannot use the same port number to configure the next Syslog connector, you should provide any other port number which is mentioned above

Step 4

Enable the connectivity between the End Device and the Connector server.

Here we can use the ping command to check the connectivity on both directions.

Step 5

Make sure that the respective Port Number is open between end device and connector server if there is a firewall in between.

If it is not open then we can contact firewall team to open the port number that we configured on the connector (514……519, or 1024 +)

Step 6

Configure the connector server details such as IP address, Port number and protocol on the End Device in order to forward the logs.

These things we can send to the respective end device configuration team, along with the steps to configure the end devices; it is called **Log Baseline Document**.

Step 7

The final step is to verify whether the logs are coming or not.

This can be done by logging into the Logger and ESM, then enter the query

" **Device Address= <IP Address of the End Device>** "

Configuration on linux devices side:-

Step 1- We need to follow the below process to configure logs forwarding from device to connector.

We have to find out which kind of syslog is running. There are three types of syslog. One of the following syslog might be available on your system.

- syslogd
- rsyslogd
- syslog-ng

Step 2

1- Log in as “root” user.

2. “ps -elf | grep -i syslog” will show which syslog is running on system.

```
McAfee-ETM-VM4 ~ # ps -elf | grep -i syslog
5 S root       678     1  0  80   0 -   601 poll_s Aug06 ?        00:00:00 syslogd
```

Figure 1. Example of a system where "syslogd" is running.

```
[root@localhost ~]# ps -elf | grep -i syslog
5 S root       852     1  0  80   0 - 62272 poll_s 10:07 ?
/rsyslogd -i /var/run/syslogd.pid -c 5
```

Figure 2. Example of a system where "rsyslog" is running

```
ict@db-vm:~$ ps -elf | grep -i syslog-ng
0 S root      2834     1  0  80   0 - 19119 -      10:28 ?        00:00:00 /usr/sbin/
0 S ict       2893  1334  0  80   0 -  3555 pipe_w 10:28 pts/0    00:00:00 grep --col
ict@db-vm:~$
```

Figure 3. Example of a system where "syslog-ng" is running

Step 3

Depending on type of syslog availability follow one of the instructions below to find out the location of configuration file of syslog. (Optional step, if configuration file is not in standard path)

i. find / -name “syslog.conf”

```
McAfee-ETM-VM4 ~ # find / -name "syslog.conf"
/etc/syslog.conf
McAfee-ETM-VM4 ~ #
```

ii. find / -name “rsyslog.conf”

```
[root@localhost ~]# find / -name rsyslog.conf
/usr/share/dracut/modules.d/98syslog/rsyslog.conf
/etc/rsyslog.conf
[root@localhost ~]#
```

iii. find / -name “syslog-ng.conf”

```
ict@db-vm:~$ sudo find / -name "syslog-ng.conf"
[sudo] password for ict:
/etc/syslog-ng/syslog-ng.conf
```

Step 4 Following one of the instructions below is configuration depending on syslog availability of the system.

a. For syslogd

i. Log on to the Linux device as “root” user.

ii. Enter the command - **vi /etc/syslog.conf** to open the configuration file called **syslog.conf**.

iii. Enter *.* and press the Tab key and enter the name of the host machine where the server is running.

. @@10.0.12.164

iv. /etc/rc.d/init.d/syslog restart

b. For rsyslog

i. Log on to the Linux device as “root” user.

ii. Enter the command - vi /etc/rsyslog.conf to open the configuration file called rsyslog.conf.

iii. *.* @@10.0.12.164:514

iv. service rsyslog restart

c. For syslog-ng

i. Log on to the Linux device as “root” user.

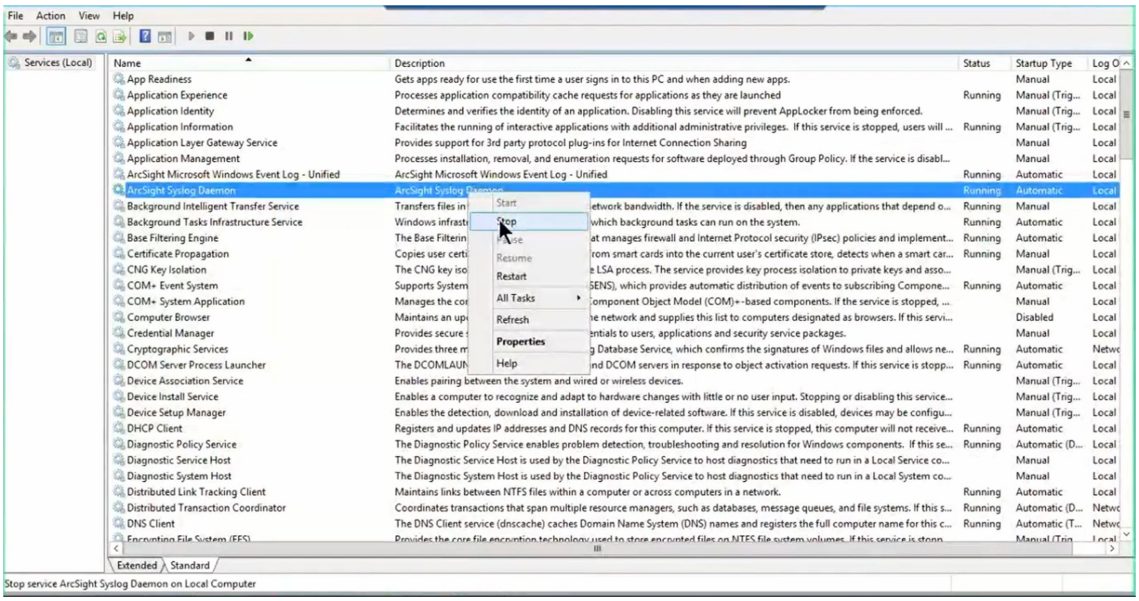
ii. Enter the command - vi /etc/syslog-ng/syslog-ng.conf to open the configuration file called “syslog-ng.conf” to add following lines. source s_local { system(); internal(); } destination siem_host_tcp { network("10.0.12.164" transport("tcp") port(514)); }; log { source(s_local); destination(siem_host_tcp) }

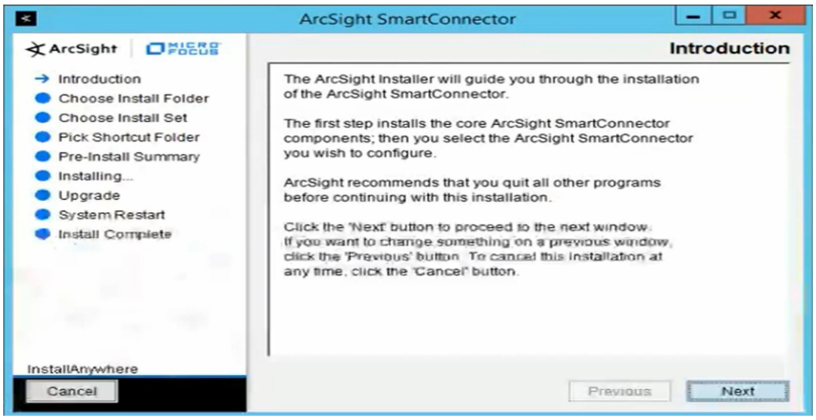
iii. service syslog-ng restart

Connector Upgradation Step by Step:-

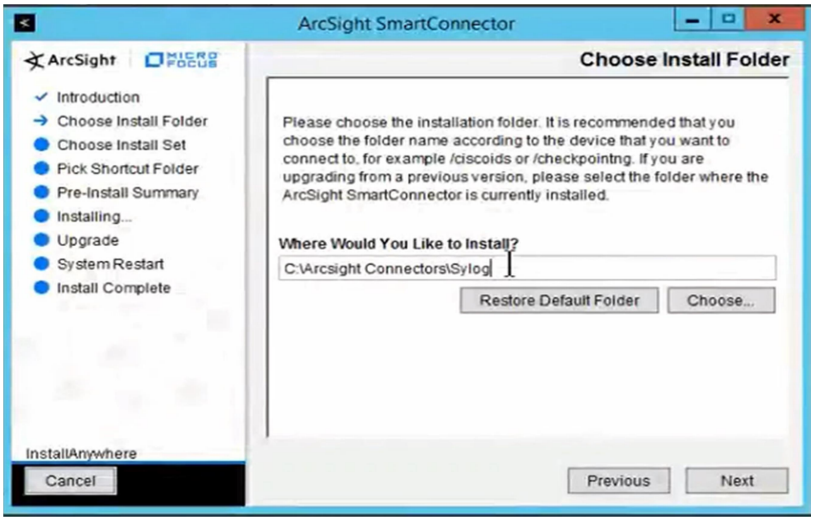
To upgrade connector locally, we will follow below steps

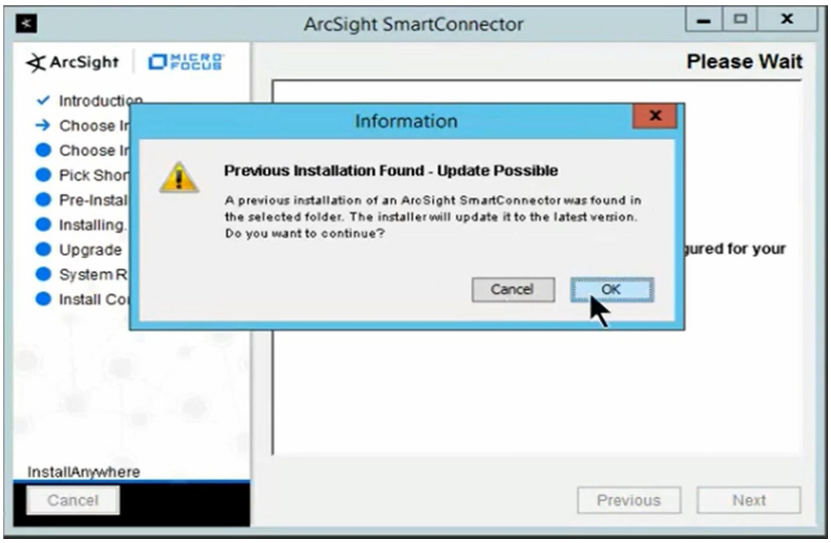
Step 1: Stop the running connector and run the new Smart Connector installer as "**Run as administrator**". The installer prompts you for the location to install the connector.



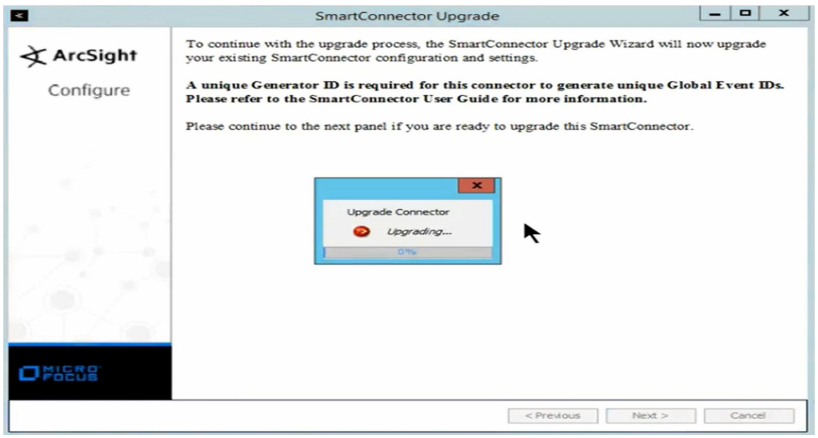


Step 2: Select the location of the Smart Connector that you want to upgrade. The message "**Previous Version Found". Do you want to upgrade?**" appears.

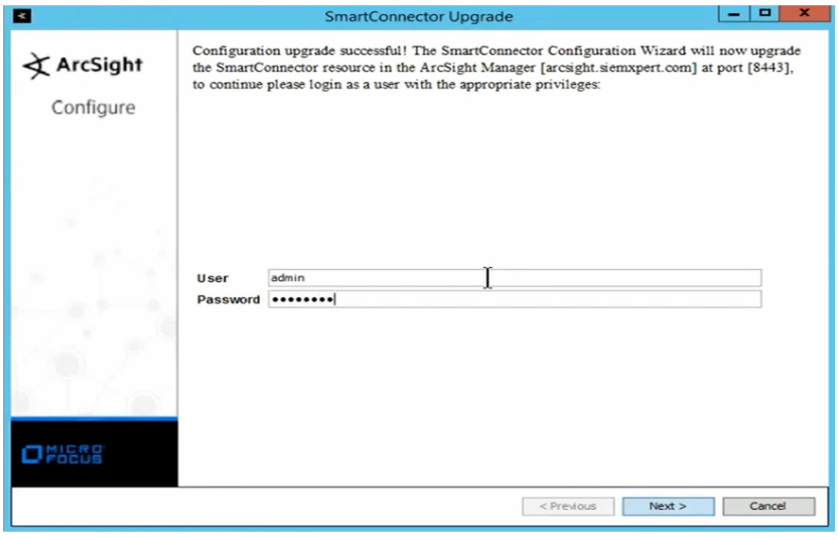




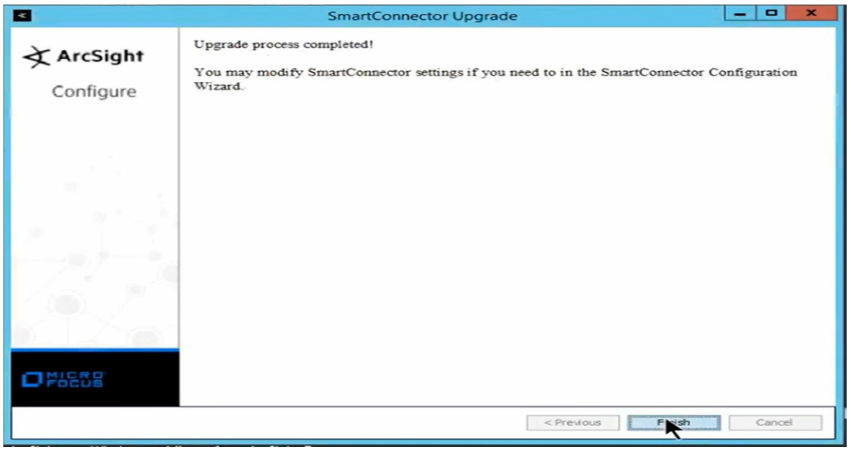
Step 3: Select the option to continue and upgrade the connector. The original installation is renamed by prefacing characters to the original folder name; the upgraded connector is installed in the location \$ARCSIGHT_HOME\current.



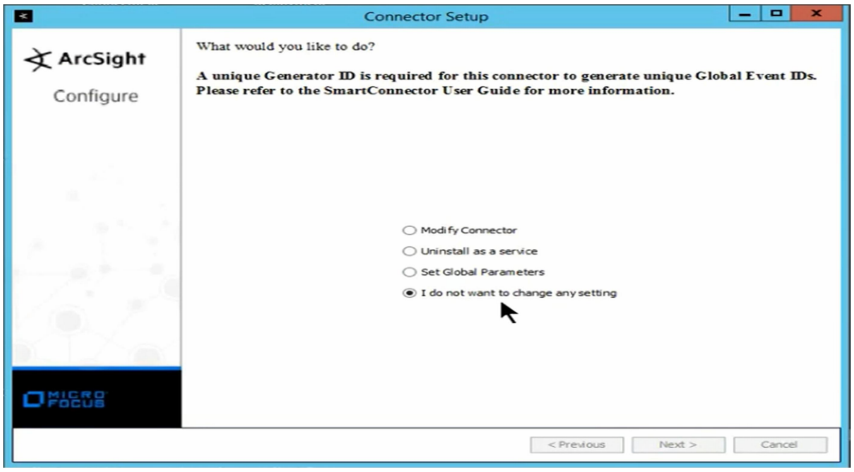
Provide ESM username and password as below and then **Next**.



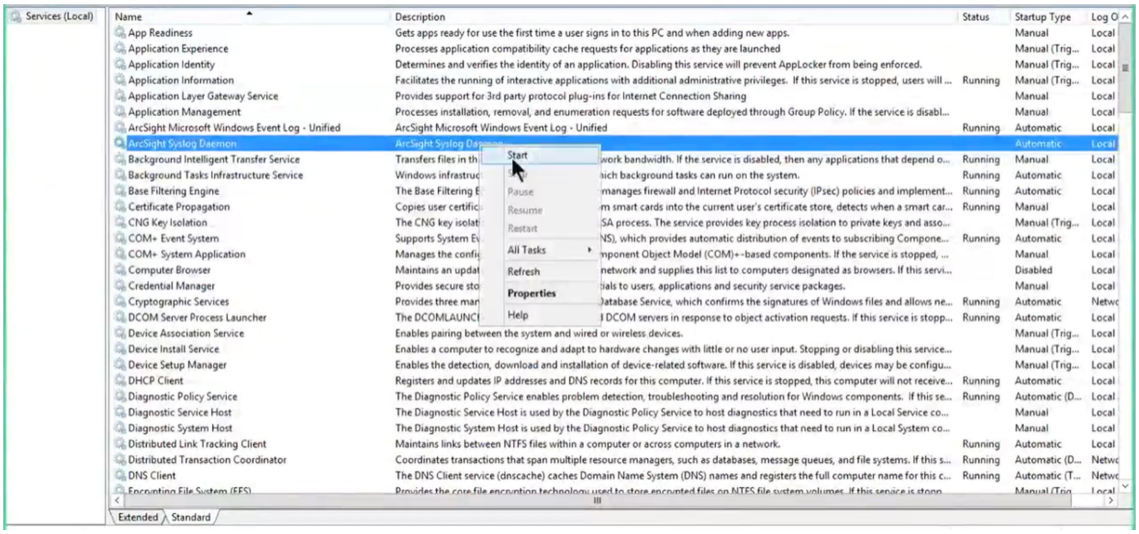
It will upgrade the connector so **Finish** the wizard.



Select "**I do not want to change any setting**" then **Next** and exit.



Step 3: Start the connector service & check the latest agent.log & agent.wrapper.log to confirm successful Connector up-gradation.



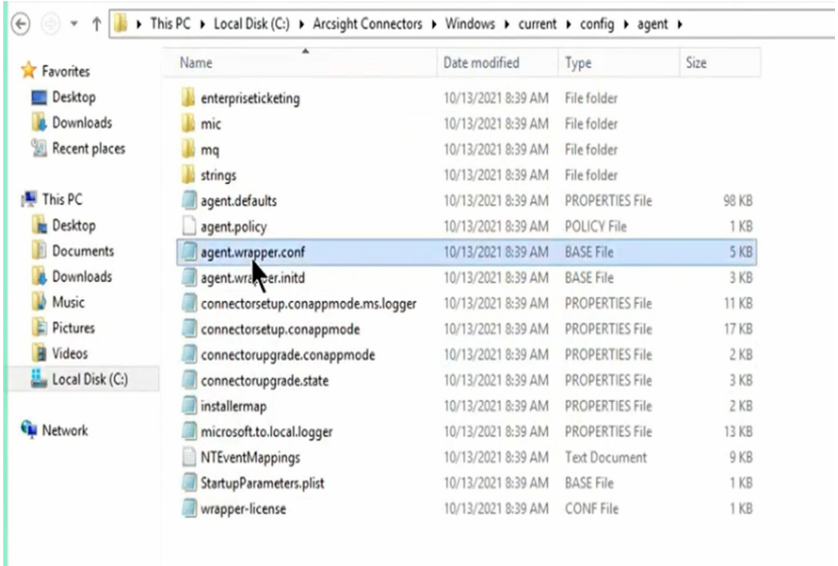
How to Increase the JVM of Connector:-

As default JVM is 256 MB. Suppose we want to increase windows connector's JVM.

Step 1 - First we will stop the connecter service.

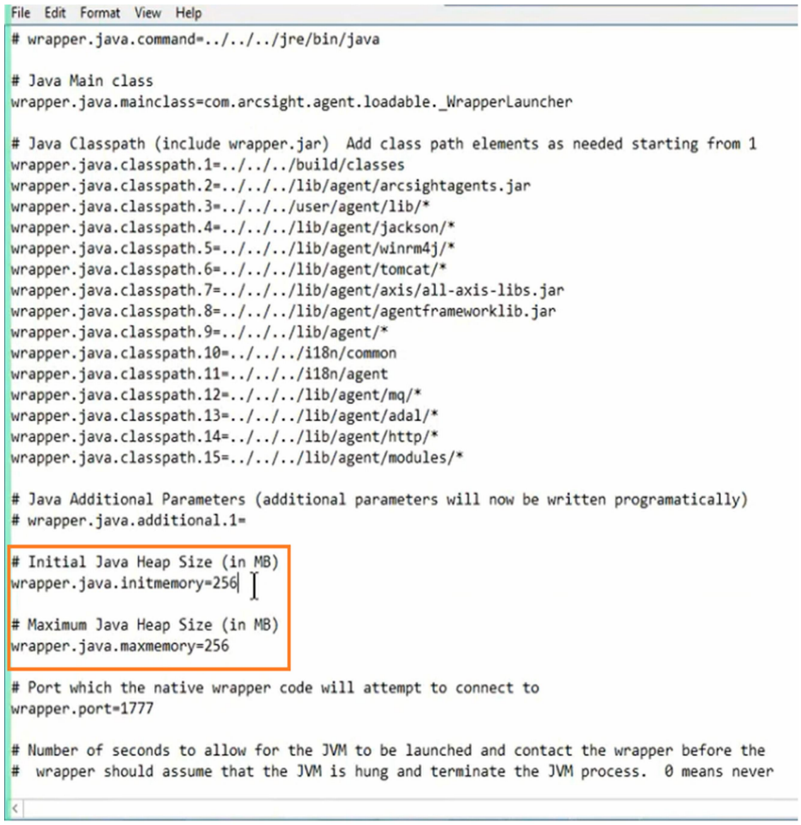
Step 2 - Browse connector folder where it is installed

ie: **C:\ drive -> current -> config -> agent** and right click on agent.wrapper.conf -> open in notepad.



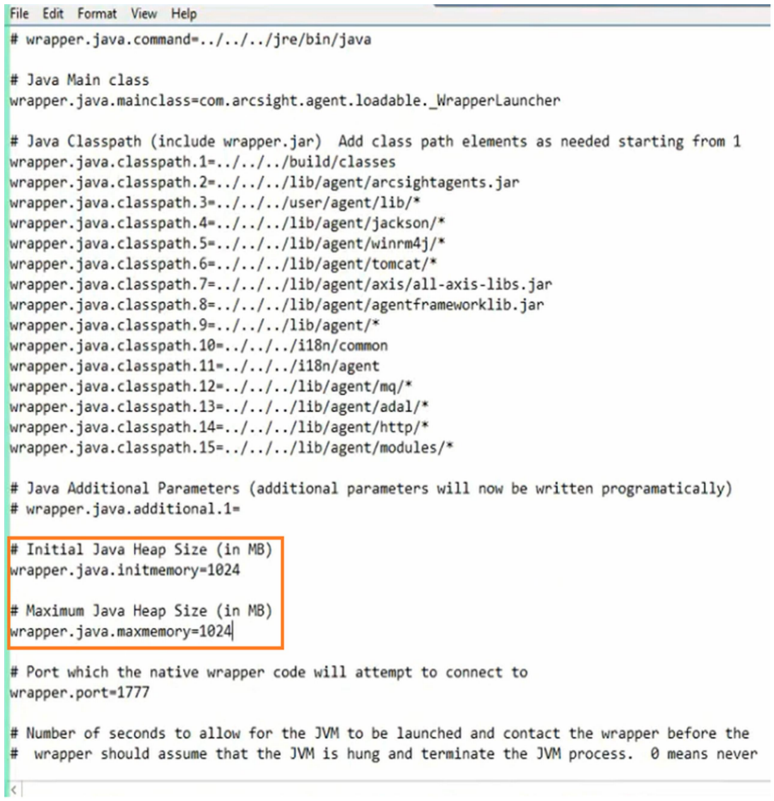
Step 3 - Navigate to the line-

" #Initial Java Heap Size (In MB)
Wrapper.java.initmemory=256
#maximum Java Heap Size (In MB)
Wrapper.java.maxmemory=256" as below.



And change it as required

" #Initial Java Heap Size (In MB)
Wrapper.java.initmemory=1024
#maximum Java Heap Size (In MB)
Wrapper.java.maxmemory=1024" as below.



```
File  Edit  Format  View  Help
# wrapper.java.command=../../../jre/bin/java

# Java Main class
wrapper.java.mainclass=com.arcsight.agent.loadable._WrapperLauncher

# Java Classpath (include wrapper.jar)  Add class path elements as needed starting from 1
wrapper.java.classpath.1=../../../build/classes
wrapper.java.classpath.2=../../../lib/agent/arcsightagents.jar
wrapper.java.classpath.3=../../../user/agent/lib/*
wrapper.java.classpath.4=../../../lib/agent/jackson/*
wrapper.java.classpath.5=../../../lib/agent/winrm4j/*
wrapper.java.classpath.6=../../../lib/agent/tomcat/*
wrapper.java.classpath.7=../../../lib/agent/axis/all-axis-libs.jar
wrapper.java.classpath.8=../../../lib/agent/agentframeworklib.jar
wrapper.java.classpath.9=../../../lib/agent/*
wrapper.java.classpath.10=../../../i18n/common
wrapper.java.classpath.11=../../../i18n/agent
wrapper.java.classpath.12=../../../lib/agent/mq/*
wrapper.java.classpath.13=../../../lib/agent/adal/*
wrapper.java.classpath.14=../../../lib/agent/http/*
wrapper.java.classpath.15=../../../lib/agent/modules/*

# Java Additional Parameters (additional parameters will now be written programatically)
# wrapper.java.additional.1=

# Initial Java Heap Size (in MB)
wrapper.java.initmemory=1024

# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024

# Port which the native wrapper code will attempt to connect to
wrapper.port=1777

# Number of seconds to allow for the JVM to be launched and contact the wrapper before the
#  wrapper should assume that the JVM is hung and terminate the JVM process.  0 means never
```

Step 4 - Restart the connector service in services.

ArcSight Lab

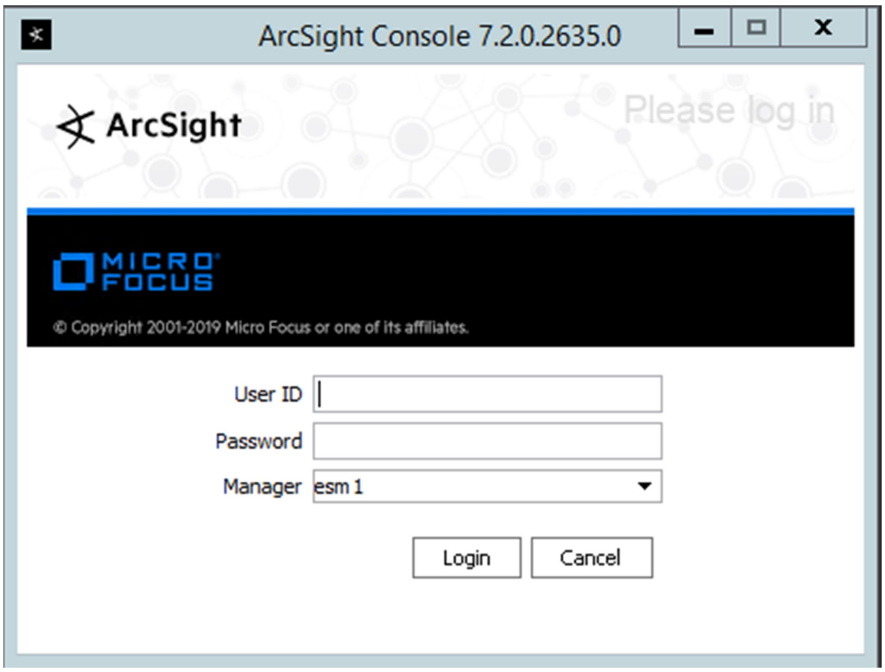
ArcSight:

We can access ESM by two ways.

1- ESM Console
2- Command Center

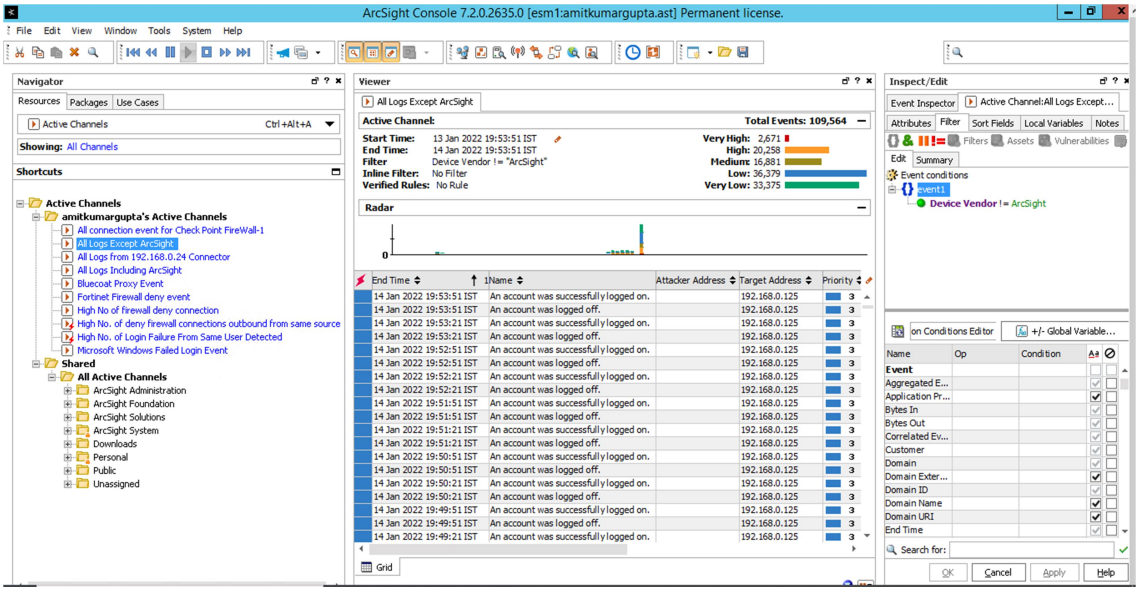
ESM Console:

3- ESM Console is the user interface by which we can access ESM. Like below-

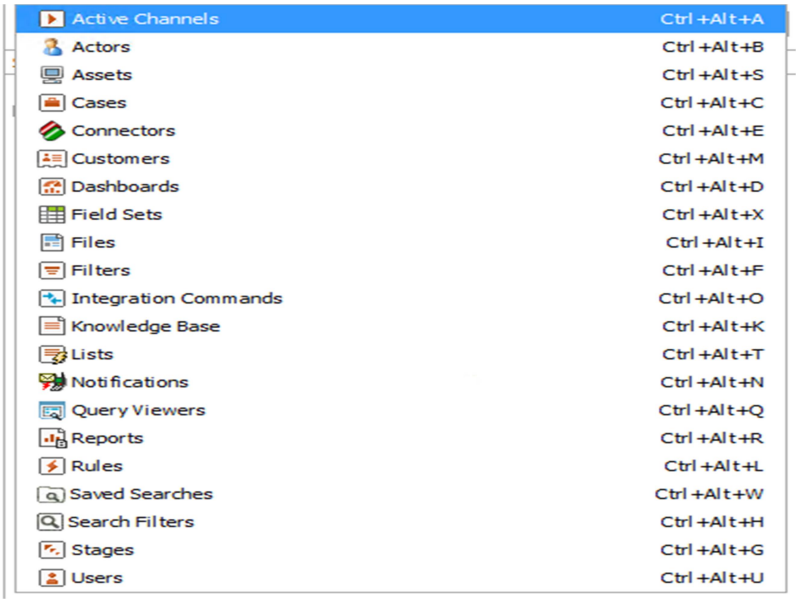


There are three panels in ESM Console.

1- Navigator- It further has three tabs.
   - Resource,
   - Package and
   - Use Cases.
2- Viewer
3- Inspect/Edit



Resource: There are 21 resources available.



1- **Active Channel:** Active Channels are the resource of ESM by which we can investigate the real time events and view event stream live or historical events by writing condition and also can download the events only in csv format from itself.

2- **Field Sets:** Field Sets are the resource of ESM. It is a combination of fields. Creating the Field Set is one time task. Every device has approximately 30+ field set but by default ArcSight displays only some fields. So we create a group of all those required fields for analysis purpose, is called Field Set.

There are 300+ fields are grouped together in 17 groups of Field Sets as follows.

3- Filters: Filter is another resource of the ESM. Filter is nothing but set of conditions that we have to write in many places such as rules, queries, active channel, data monitor. So instead of writing the condition manually, we can call the filter.

Inline Filter: Inline filters further refine the result of a filtered active channel.

4- Query Viewer: Query viewer is a resource of ESM which displays the result of queries in order to get real time events or historical events by defining condition, time and field set in query.

5- Reports: Report is a resource of ESM which process the queries in background of ESM and does not much impact on the resources of ArcSight. It provides option to download the result of queries in which time, condition, Field Sets are defined. Report can be download in multiple formats. ie: csv, pdf, xslx etc.

There are two ways to generate the report.

1- **Query based Report (Query -> Report)-** Whenever we run the report based on query, at the same time, it goes to database and search the log based on defined query.

2- **Trend based Report (Query -> Trend -> Report)-** Whenever we run the report based on trend, we schedule the trend and at the scheduled trend, it goes to database, search the log based on defined query and save it to trend table in database. After it when we run the report, it immediately it downloads the report from the trend table.

6- Rules: Rule is a resource of ESM. Rule is nothing but set of conditions along with aggregation.

When we correlate it with each other, it is called correlation rule.

There are three type of rule.

1- Standard Rule

2- Lightweight Rule

3- Pre-persistence Rule

Fine Tune of Rule- Doing the necessary changes on the rule condition or aggregation to insure that maximum time the rule will trigger only in case any suspicious activity found.

We can do fine tune by-

1- Increasing or decreasing the aggregation

2- Changing the rule condition or Whitelisting certain condition to avoid false positive alert.

3- Applying suppression or delay list to avoid repetitive rule firing.

4- Avoid partial matches of the rules by decreasing the aggregation.

7- List or Active List: Active Lists are resources of the ESM that store event data/fields (not entire events) for a definite or indefinite period of time.

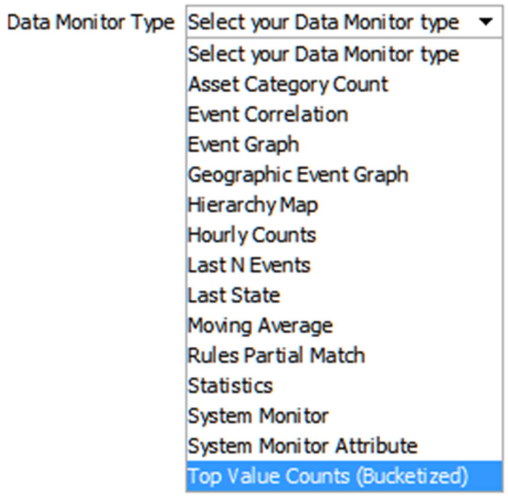
We have two kind of Active List:

- **Event based Active List-** In event based active list, during the creation of active list, we define only ArcSight defined fields and can use for that purpose only for which it is being created. It is less resource intensive.
- **Field Based Active List-** In field based active list it provide flexibility while creating active list, we can give it own name and use for multiple purposes. Once we call it to the rule we map with the ArcSight defined fields. It is less resource intensive.

8- Stages: Stage is a resource of ESM. Stages are nothing but state of the events which is set by the analyst by annotating events from the main channel and setting them to various level of investigation. Ie: Queued, In-Progress, Follow-up or Closed.

9- Dashboard: Dashboard is another resource of ESM which enables visualization of Real-time event monitoring and correlation with data from ArcSight Enterprise Security and helps us to identify, and analyse potential threats.

To create a dashboard, first we will create Data Monitor which is as follows:-



High Severity Daily incidents

1- High No Windows login failure attempt detected.
2- High no of UNIX login failure attempt detected.
3- High no of deny firewall traffic inbound/outbound.
4- Successful connection from blacklisted IP.
5- Successful Brute force attacks.
6- Successful connection towards blacklisted IP.
7- Traffic from Trojan port/malware ports. Rule for Allowed event only.
8- Traffic towards Trojan port/malware ports. Rule for Allow & Deny both.
9- Torrent traffic detected.
10-Symantec antivirus detected malware.

What is Threat Feeds- Set of IPs, Urls, Domains, emails, etc. which are blacklisted due to involvement in suspicious activity.

IOCs (Indicators of Compromise)- Set of IPs, Urls, Domains, emails etc. which are recently used in malicious activities is called IOCs.

ArcMC - ArcSight Management Center (ArcMC) is a centralized security management centre that is used to manage large/multiple deployments of ArcSight solutions such as ArcSight Connector, ESM & Logger through a centralized management console. We can upgrade the components and can back up of all these components.